IS150

Smart Security

Web User's Manual

v.1.0

May, 2013

Important Announcement

The information contained in this document is the property of Atop Technologies, Inc., and is supplied for the sole purpose of operation and maintenance of Atop Technologies, Inc. products. No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of Atop Technologies, Inc., offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome. All other product names referenced herein are registered trademarks of their respective companies.

Published by

Atop Technologies, Inc.

2F, No. 146, Sec. 1, Tung-Hsing Rd.
Jubei, Hsinchu 30261
Taiwan, R.O.C.
Tel: 886-3-5508137
Fax: 886-3-5508131
www.atop.com.tw
www.atop-tech.com

Copyright © 2013 Atop Technologies, Inc. All rights reserved. Technical data is subject to change. All other product names referenced herein are registered trademarks of their own respective companies.

Contents

1 Preface 5

2 Introduction 8

2.1 Product Overview 8
2.2 Features 10

3 Getting Started 11

3.1 Model Comparison 11
3.2 First Time Installation 11
3.3 Finding the device 11
3.4 Factory Default Settings 13

4 Web Configuration 15

4.1 Web Configuration Overview 15
4.2 Operation Modes 17
4.2.1 Regular AP Gateway Mode 17
4.2.2 AP Client Mode 19
4.3 System Information 22
4.3.1 Device Information 22
4.3.2 LAN Information 22
4.3.3 DI/DO Information 23
4.3.4 Wireless Information 23
4.3.5 GPRS/UMTS Information 24
4.3.6 Wireless Client Table (Regular AP Gateway Mode) 24
4.3.1 DHCP Client Table (Regular AP Gateway Mode) 25
4.4 Network Settings 26
4.4.1 LAN (Regular AP Gateway Mode) 26
4.4.2 Local Area Network (AP Client Mode) 27
4.4.3 WAN (Regular AP Gateway Mode) 29
4.4.4 Virtual Server (Regular AP Gateway Mode) 30
4.4.5 SNMP Settings 31
4.4.6 DHCP Server (Regular AP Gateway Mode) 32
4.5 Wireless Settings 33
4.5.1 Secure Wireless Wi-Fi Network 33

4.5.2 Basic Settings (Regular AP Gateway) 34
4.5.3 Mobile Station (AP Client) 40
4.5.4 Security Settings (Regular AP Gateway Mode) 43
4.5.5 Advanced Settings 46
4.6 Input / Output 48
4.7 System Setting 49
4.7.1 Firmware Upgrade 49
4.7.2 Time 50
4.7.3 Password 51
4.7.4 Restore to Default 52
4.7.5 Reboot 53
4.8 Logout 53

5 WAN Configuration 54

5.1 PPPoE 54
5.2 DHCP 56
5.3 Static IP 57
5.4 GPRS/UMTS 58
5.4.1 Enabling the SIM card 58
5.4.2 List of Compatible Internet Service Providers (ISP) 61
5.5 LED Indicators 62

6 Warranty 63

1 Preface

Purpose of the Manual

This manual supports you during the installation and configuring of the IS150 Smart Security Server only, as well as it explains some technical options available with the mentioned product. As such, it contains some advanced network management knowledge, instructions, examples, guidelines and general theories designed to help users manage this device and its corresponding software; a background in general theory is a must when reading it. Please refer to the Glossary for technical terms and abbreviations (if any).

Who Should Use This User Manual

This manual is to be used by qualified network personnel or support technicians who are familiar with network operations; it might be useful for system programmers or network planners as well. This manual also provides helpful and handy information for first time users. For any related problems please contact your local distributor, should they be unable to assist you, please redirect your inquiries via www.atop.com.tw or www.atop-tech.com.

Supported Platform

This manual is designed for the IS150 Smart Security Server and that model only.

Warranty Period

We provide a **3 year limited warranty** for IS150 Smart Security Server.

Manufacturers Federal Communication Commission Declaration of Conformity Statement
Model: IS150

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.
FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
This device is restricted to indoor use when operated in the 5.15 to 5.25 GHz frequency range.

※ FCC requires this product to be used indoors for the frequency range 5.15 to 5.25 GHz to reduce the potential for harmful interference to co-channel Mobile Satellite systems.

FCC Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator & your body.

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Model: IS150

Declaration of Conformity with regard to the R&TTE Directive 1999/5/EC

This equipment is in compliance with the essential requirements and other relevant provisions of 1999/5/EC.

The following standards were applied:

EMC EN 301.489-1 v1.4.1; EN 301.489-17 v1.2.1

Health & Safety EN60950-1: 2001; EN 50385: 2002

Radio EN 300 328 v 1.7.1; EN 301.893 v 1.5.1

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

This device also conforms to the EMC requirements of the Medical Devices Directive 93/42/EEC.

Note: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact Atop Technical Support.

European Union

This system has been evaluated for RF exposure for humans in reference to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The evaluation was based on the EN 50385 Product Standard to Demonstrate Compliance of Radio Base stations and Fixed Terminals for Wireless Telecommunications Systems with basic restrictions or reference levels related to Human Exposure to Radio Frequency Electromagnetic Fields from 300 MHz to 40 GHz. The minimum separation distance from the antenna to a general bystander is 20 cm (7.9 inches).

2 Introduction

2.1 Product Overview

The **IS150 Smart Security Server** series is our new line of security products designed to allow remote access through its rich wired and wireless interfaces creating a complete solution for your home and/or store security and surveillance needs.

As an example, you can connect multiple sensors and detectors to IS150 using its digital input interface and connect alarms to IS150 using its digital output interfaces; this example illustrates a typical security system guarded by IS150, Figure 2.1.

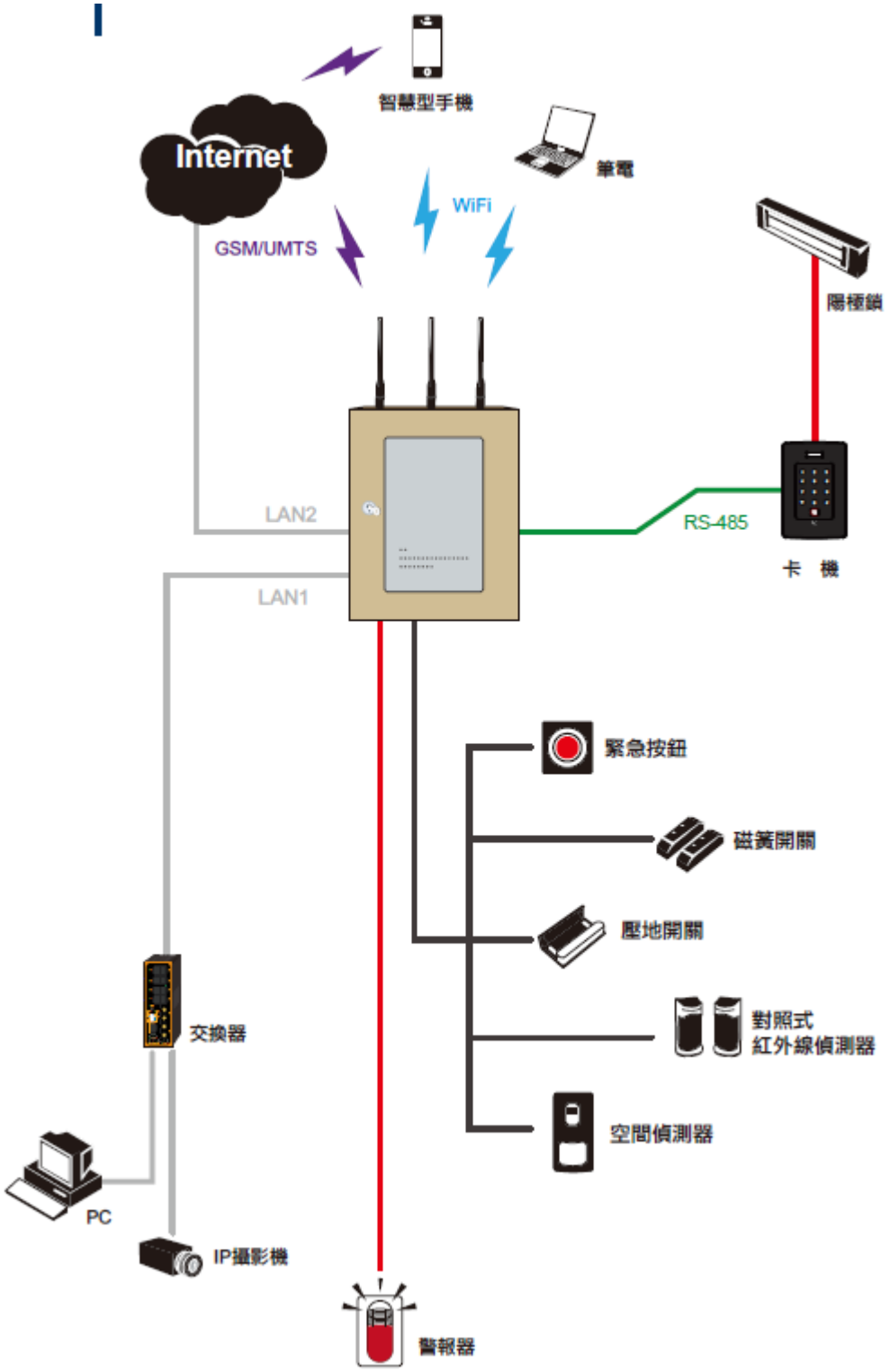

智慧型手機
Internet
筆電
WiFi
GSM/UMTS
陽極鎖
LAN2
RS-485
卡 機
LAN1
緊急按鈕
磁簧開關
壓地開關
交換器
對照式
紅外線偵測器
空間偵測器
PC
IP攝影機
警報器

Figure 2.1

2.2 Features

IS150 is our latest addition to our smart security products; its powerful architecture makes it a perfect choice for business/home needs in which security is a decisive factor. It rewards our customers with superb connectivity. Among its many characteristics, we could mention:

- Send alarm messages through email or SMS
- Provide 8-Door access control
- Monitor sites using IP Camera from anywhere in the world
- 16 sets of independent digital inputs and 8 digital outputs for variety of uses
- Provide iOS / Android / Windows / Web interfaces for monitor and configuration
- Watchdog protected to recover from system crash

3 Getting Started

3.1 Model Comparison

Table 3.1

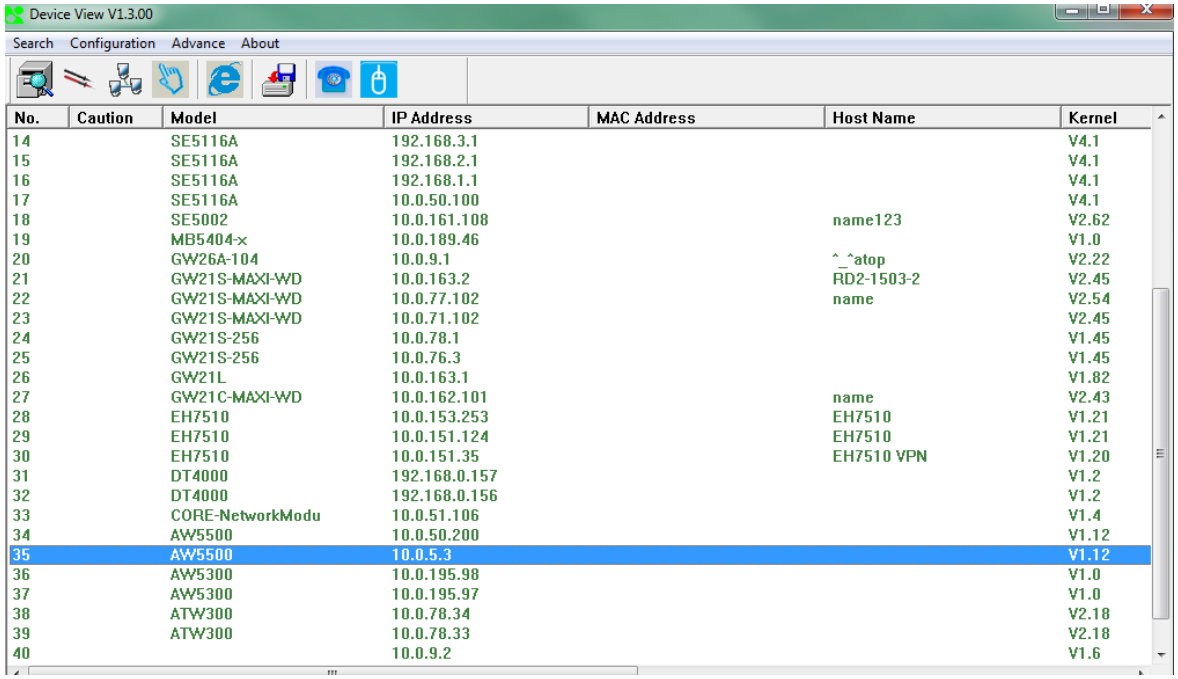
Model	Description
IS150-WG	Smart Security Server with WCDMA and WiFi module
IS150-G	Smart Security Server with WCDMA module only
IS150-W	Smart Security Server with WiFi module only
IS150	Smart Security Server without any wireless function

3.2 First Time Installation

Please consult your Hardware Installation Guide when attempting the installation. Also, please follow all safe procedures when doing so.

3.3 Finding the device

As soon as the device is connected to the network, the user can search for its IP settings using **Device View ©,** (utility that comes in the CD); as noted in Figure 3.1 below, important information such as the IP, MAC address, etc is going to be displayed.



No.	Caution	Model	IP Address	MAC Address	Host Name	Kernel
14		SE5116A	192.168.3.1			V4.1
15		SE5116A	192.168.2.1			V4.1
16		SE5116A	192.168.1.1			V4.1
17		SE5116A	10.0.50.100			V4.1
18		SE5002	10.0.161.108		name123	V2.62
19		MB5404-x	10.0.189.46			V1.0
20		GW26A-104	10.0.9.1		^_^atop	V2.22
21		GW21S-MAXI-WD	10.0.163.2		RD2-1503-2	V2.45
22		GW21S-MAXI-WD	10.0.77.102		name	V2.54
23		GW21S-MAXI-WD	10.0.71.102			V2.45
24		GW21S-256	10.0.78.1			V1.45
25		GW21S-256	10.0.76.3			V1.45
26		GW21L	10.0.163.1			V1.82
27		GW21C-MAXI-WD	10.0.162.101		name	V2.43
28		EH7510	10.0.153.253		EH7510	V1.21
29		EH7510	10.0.151.124		EH7510	V1.21
30		EH7510	10.0.151.35		EH7510 VPN	V1.20
31		DT4000	192.168.0.157			V1.2
32		DT4000	192.168.0.156			V1.2
33		CORE-NetworkModu	10.0.51.106			V1.4
34		AW5500	10.0.50.200			V1.12
35		AW5500	10.0.5.3			V1.12
36		AW5300	10.0.195.98			V1.0
37		AW5300	10.0.195.97			V1.0
38		ATW300	10.0.78.34			V2.18
39		ATW300	10.0.78.33			V2.18
40			10.0.9.2			V1.6

Figure 3.1

If the device's name is double-clicked or the Internet Explorer logo is clicked, **Device View** would open the Web UI of IS150 using the system default browser. A window will pop-out that will prompt you to enter username and password (see **Factory Default Settings** for more information), proceed then to click **"OK",** Figure 3.2. If credentials are entered correctly, the Web UI can then be accessed.

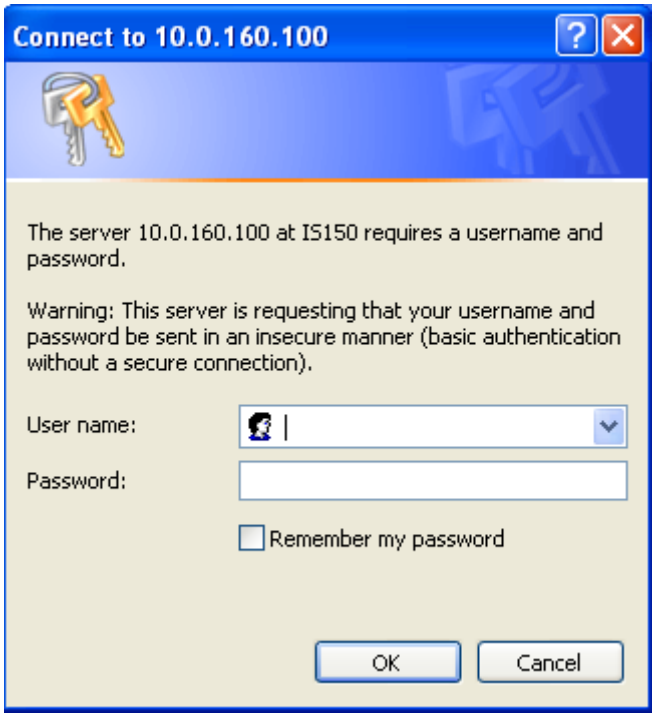

Connect to 10.0.160.100
The server 10.0.160.100 at IS150 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel

Figure 3.2

3.4 Factory Default Settings

Upon arrival, the device will be set as Regular AP, the rest of the settings are as follow:

Table 3.2

Operation Mode	**Regular AP Gateway**	**AP Client**
Network		
LAN Interface		
IP Address	10.0.50.100	N.A.
Subnet Mask	255.255.0.0	
WAN Setting		
PPPoE	Enabled	N.A.
Dial when boot up	Enabled	
Username	Blank	
Password	Blank	
Virtual Server	Disabled	
SNMP Setting		
System Contact	Contact	
System Location	Location	
System Name	Device’s MAC address	
Read Community	Disabled	
Write Community	Disabled	
DHCP Server		
DHCP	Disabled	N.A.
Wireless		
Basic Setting		
Radio Off	Disabled	N.A.
SSID	IS150	
SSID Broadcast	Enabled	
Wireless Mode	802.11 b/g/n	
Channel	Auto	
BandWidth	40MHz	
Secondary Channel	Disabled	
Transmit Rate	Disabled	

Security Setting		
Security Mode	Disabled	N.A.
Mobile Station		
Radio On/Off	N.A.	Enabled
Topology		Infrastructure
Band mode		Disabled
TxRate		Best (auto)
Channel		Disabled
BandWidth		
Secondary Channel		
Authentication Mode		OPEN
Encryption Type	N.A.	NONE
Advanced Setting		
Regulatory Domain	US(FCC5-FCCA)	
Tx Power	100%	
Short GI	Enable	
WMM	Enable	
STP	Disabled	
Input/ Output		
DI/O Setting		
DO 1	Off	
DO 2	Off	
System Setup		
Time		
Current Date/Time	Time from NTP Server	
NTP	Enabled	
NTP Server	pool.ntp.org	
Time Zone	(GMT+08:00) Taipei	
Password		
User name	admin	
Old password	Blank	
New password		
Repeat new password		

4 Web Configuration

4.1 Web Configuration Overview

IS150 Series' Web Configuration is designed into two different modes for ease of use to suit customer needs. The Web Configuration appears as follows, Figure 4.1.

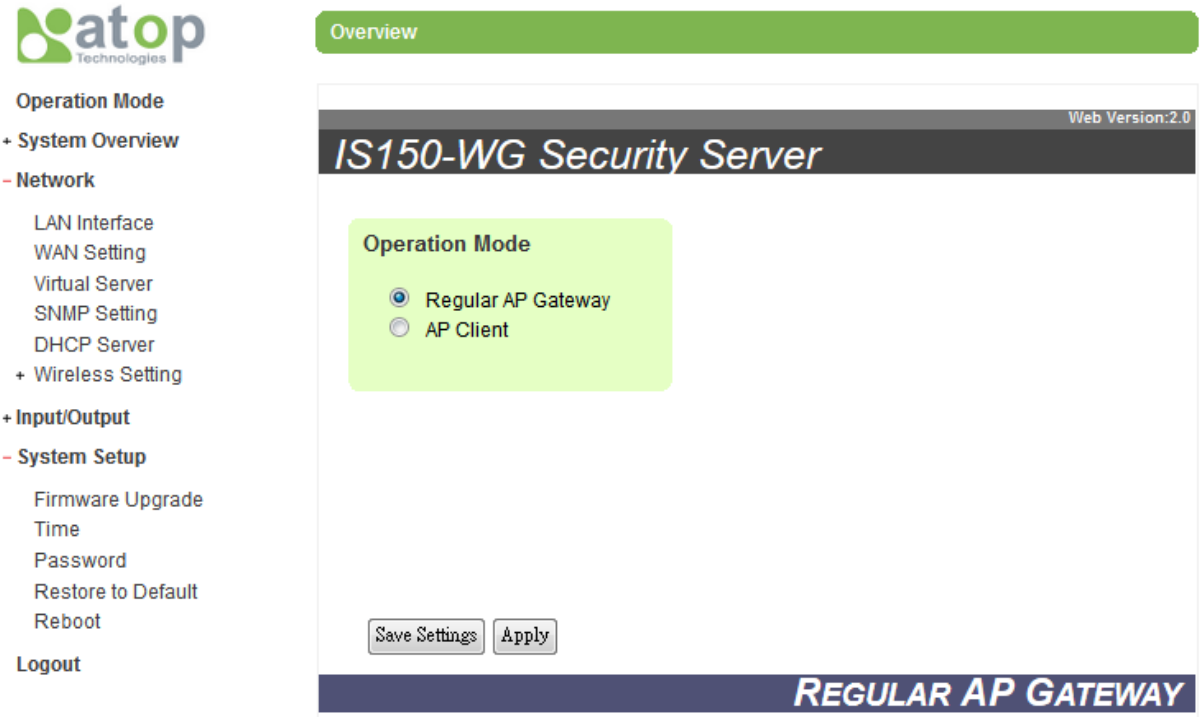


Figure 4.1

On the left side, a menu-tree appears with all the modes and options available, while on the right side of your screen the contents of each mode/option will be displayed in a graphical state. Since each Mode of operation is different, the content will differ, for more information on each selection please refer to each option's Section throughout the manual.

In general, there will be three buttons which will be present at the end of almost each configuration:

Table 4.1

Button	Function
Save Settings	Saves the current configuration input on the page only, the configuration itself will not be applied to the device. We recommend users to use this button before the configuration process is completed and then press “Apply” at the last step.
Apply	Save and apply the current configuration input on the page. On some pages, the device may need to reboot, we strongly advise to save the device’s settings before reboot.
Cancel	Cancel the current configuration input and shows the original settings.

4.2 Operation Modes

4.2.1 Regular AP Gateway Mode

Figure 4.2

Regular AP Gateway mode is the factory default and the first option on the screen. It allows network devices to connect to the network over Wi-Fi or LAN, relaying data between the wired and wireless devices in the network. It allows multiple wireless clients to access the network through IS150's WLAN interface (UMTS/PPPoE connection). Its corresponding complete menu-tree is as follows in Figure 4.3.

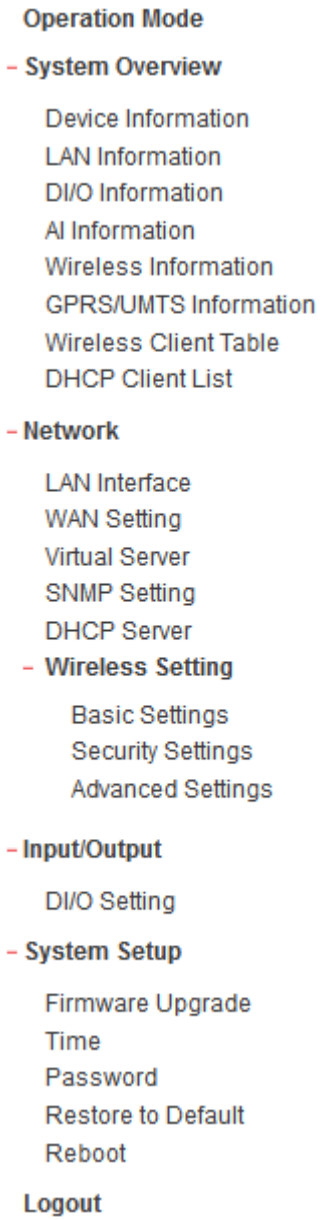


Figure 4.3

Steps for a quick setting for the IS150 as a Regular AP Gateway are:

- On operation mode choose **"Regular AP Gateway"** (if the device is not in factory default). Remember to click on **"Save"** before you continue to the next step.
- Go to **Network → LAN Settings,** enter the **IP Address, Subnet Mask** of the device
- Go to **Network → WAN Settings,** select a method that connects the device to the **Internet.**
- Go to **Network → Wireless Setting → Basic Settings;** here you can change the **Network Name** (SSID) to your preferred name, you might want to first click on **"Scan network"** to find

whether there are neighbors with a name matching yours (this is done for preventing any conflict over networks).

- At this point you may decide to change other settings such as the **Wireless Mode,** whether to have **Automatic Channel Selection,** the **Bandwidth, Transmission Rate** and the **Secondary Channel** (only available when on **802.11a/n** and **802.11b/g/n** modes).
- Next go to **Security Settings,** and on **Security Mode** choose which security protocol will be used in the network. We strongly recommend not leaving this section as disabled.
- Click **"Apply",** and wait for the changes to take effect. This will apply all the previous changes all together.

4.2.2 AP Client Mode

This mode allows your IS150 to connect to an Access Point (**AP). Ethernet clients** connected to IS150 over the Local Area Network (LAN) are allowed to access the network through IS150's wireless interface.

Figure 4.4

Its corresponding complete menu-tree is as follows in Figure 4.5.

Figure 4.5

Remember that your IS150 can function as both a **Regular AP Gateway** and as an **AP Client** (the latter connected to the first one).

Supposing we already have the network physically installed, the steps for configuring your IS150 as an **AP Client** are as follows.

- On **Operation Mode** choose **AP Client.** Click on **"Save Settings"**
- Go to **Network** → **Wireless Setting** → **Mobile Station** and click on **"Scan network"** to choose an **SSID**.
- A window/tab will pop out; in that new window/tab, there will be the names of the surrounding Wireless Networks. Choose the one that you already designated as your **Regular AP** by selecting its corresponding SSID.

- Click **"Connect",** this will make you close the pop-out window/tab, and leave you with the settings selected on the previous page.
- Enter the **WEP key** or the **WPA passphrase** if necessary.
- Scroll to the end of the page and press **"Apply",** please wait for some time for the changes to apply.
- Then proceed to go to **System Overview → Wireless Information,** you can confirm your IS150 is connected to the Network selected if the Signal field displays a signal percentage instead of disconnected. Also, you may also double check the wireless connection status inside the client table of the connected **AP.**

Wireless	
MAC Address	00:60:E9:0C:41:50
Region	US
IP Mode	Static
IP Address	10.0.50.100
Gateway	10.0.50.1
WIFI Mode	802.11b/g/n
Bandwidth	40MHz
Signal	45%

Figure 4.6

4.3 System Information

This section displays various system information for troubleshooting purposes.

4.3.1 Device Information

Device Information	
Model Name	IS150
System Name	000A48-088A3C
Kernel Version	0.04
AP Version	0.05
Operation Mode	Regular AP Gateway

Figure 4.7

4.3.2 LAN Information

LAN1 Information	
IP Address	10.0.50.100
Subnet Mask	255.255.0.0
Gateway	10.0.50.1

LAN2 Information	
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0

Figure 4.8

4.3.3 DI/DO Information

DI/O Status	
DI 1	Off
DI 2	Off
DO 1	Off
DO 2	Off

Figure 4.9

4.3.4 Wireless Information

Wireless	
MAC Address	00:60:E9:0C:41:50
Region	US
IP Mode	Static
IP Address	10.0.50.100
Gateway	10.0.50.1
WIFI Mode	802.11b/g/n
Bandwidth	40MHz
Signal	Disconnected

Figure 4.10

4.3.5 GPRS/UMTS Information

GPRS/UMTS	
Connect Status	Not Connected
IP Address	0.0.0.0
ISP Profile	Unknown
Signal	Unknown
Mode	Not registered for packet switched service
Total TX Bytes	0 Bytes
Total RX Bytes	0 Bytes

Transfer	
Upload	0 Bytes
Download	0 Bytes

Figure 4.11

4.3.6 Wireless Client Table (Regular AP Gateway Mode)

On this table you may be able to see all the wireless clients connected to IS150, Figure 4.12.

MAC Address	*AID	Channel	Tx Rate	*RSSI	Idle	Tx Seq	Rx Seq
No associated wireless client.							

*AID: Association ID.

*RSSI: Signal strength of the last received packet..

Figure 4.12

4.3.1 DHCP Client Table (Regular AP Gateway Mode)

IS150 could distribute IP addresses using the DHCP protocol; a list of clients currently receiving an IP can be accessed by choosing the DHCP Status option. DHCP Client's **MAC Address** as well as its **IP addresses**, **Host Name,** and **Lease Time** will be shown in this list, Figure 4.13.

Host Name	MAC Address	IP Address	Lease Time
No DHCP entry.			

Refresh

Figure 4.13

4.4 Network Settings

4.4.1 LAN (Regular AP Gateway Mode)

Here you can designate IS150's local IP address for LAN devices to access it, Figure 4.14. Note that this IP address is private and used locally only. To access IS150 on the Internet, follow the instructions in **WAN (Regular AP Gateway Mode)**.

Note: IS150 uses Port 1 (the lower port) as the LAN port.

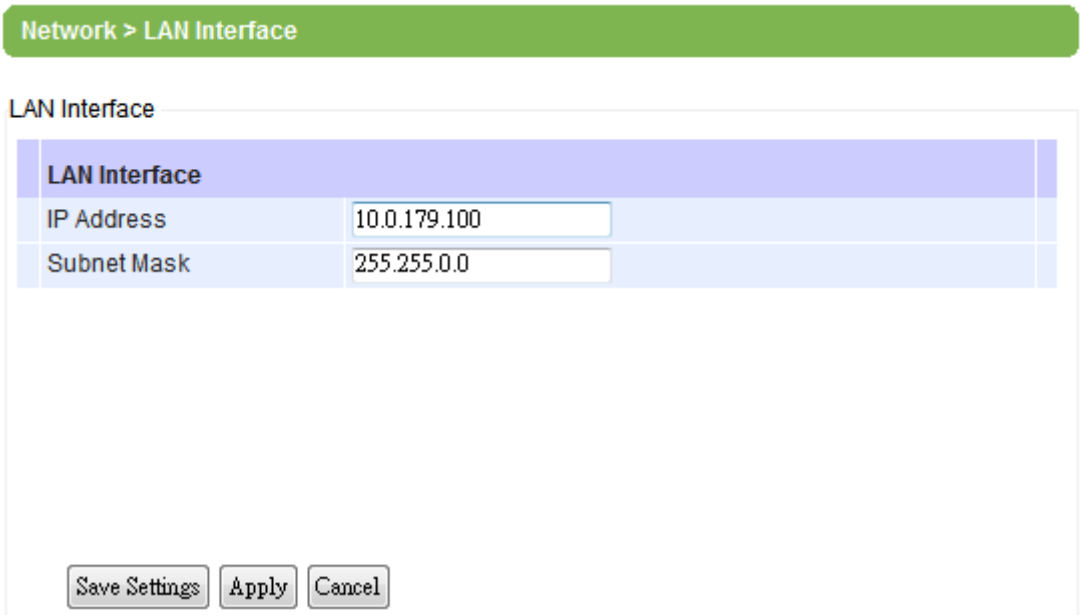


Figure 4.14

4.4.2 Local Area Network (AP Client Mode)

Under the AP Client mode, IS150 will have two LAN interfaces. LAN1 will be bridged with the Wi-Fi interface where it can access another network through IS150's Wi-Fi interface. LAN2 could be used to create a different subnet. Keep in mind that LAN1 and LAN2 are not bridged together, so they cannot talk to each other.

To get an IP address from a DHCP server connected on the LAN interface, just check **"Obtain an IP Address Automatically"** for it, Figure 4.15; or enter the values manually if known, Figure 4.16.

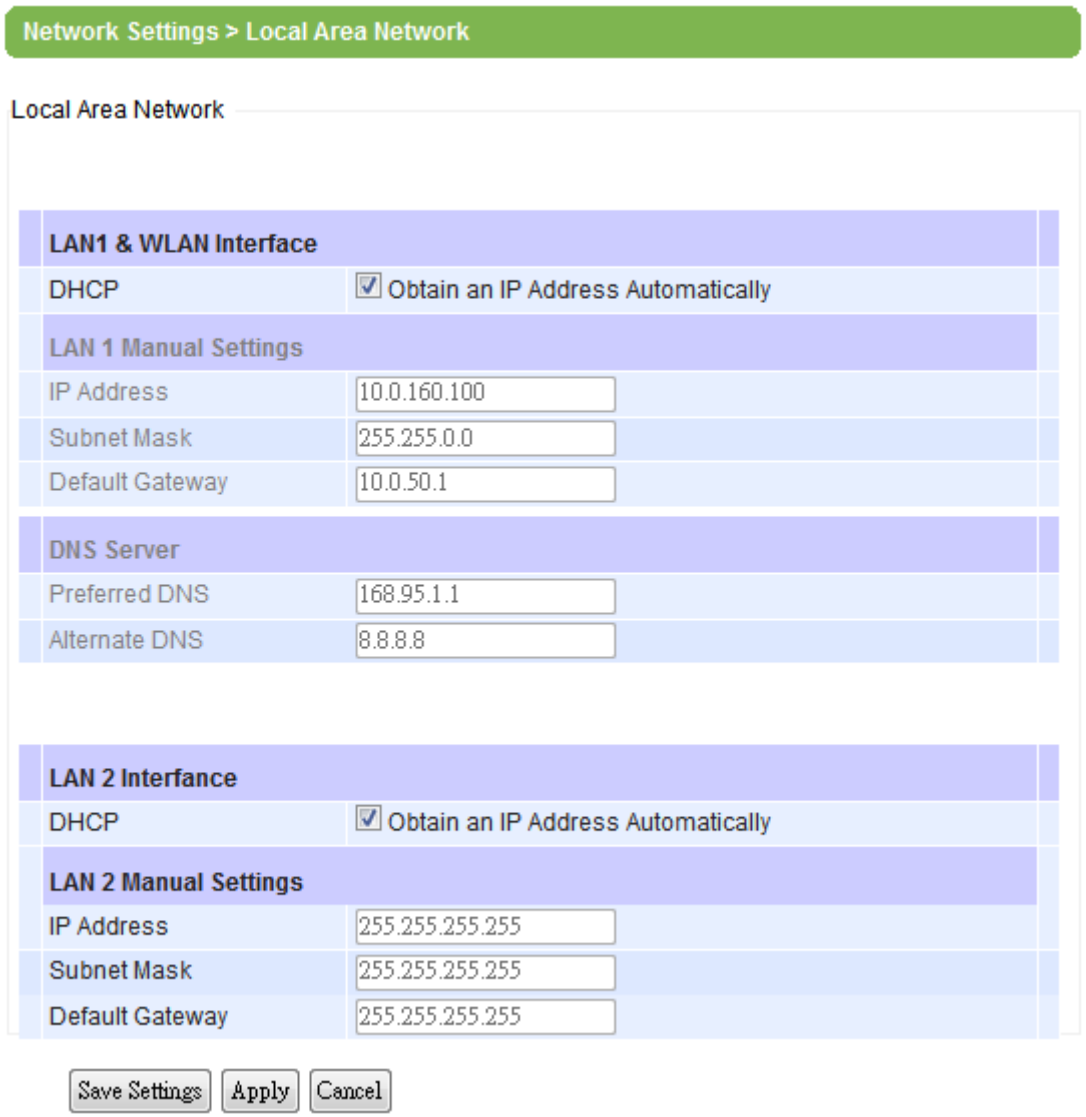


Figure 4.15

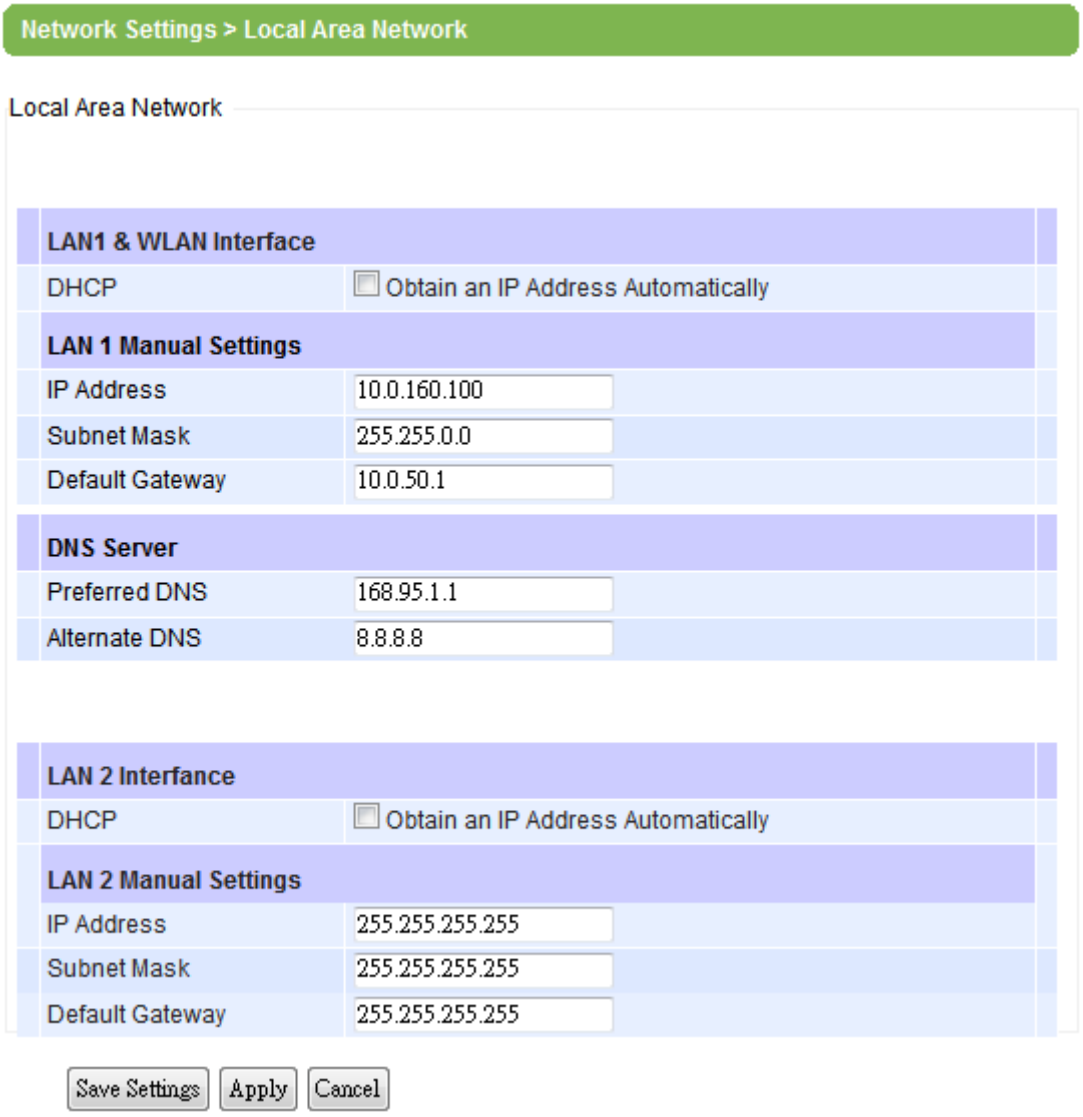


Figure 4.16

Note: IS150 uses Port 1 (the lower port) as the LAN port.

4.4.3 WAN (Regular AP Gateway Mode)

There are different ways that IS150 can connect to the Internet, which are **PPPoE, GPRS/UMTS, DHCP, and Static IP**, Figure 4.14. Each of these options assume that the Internet is setup properly at the remote/server side and IS150 only needs to connect to it in order to access the Internet. Due to the complication nature of the WAN setup, a separate chapter has been created to address **WAN Configuration**.

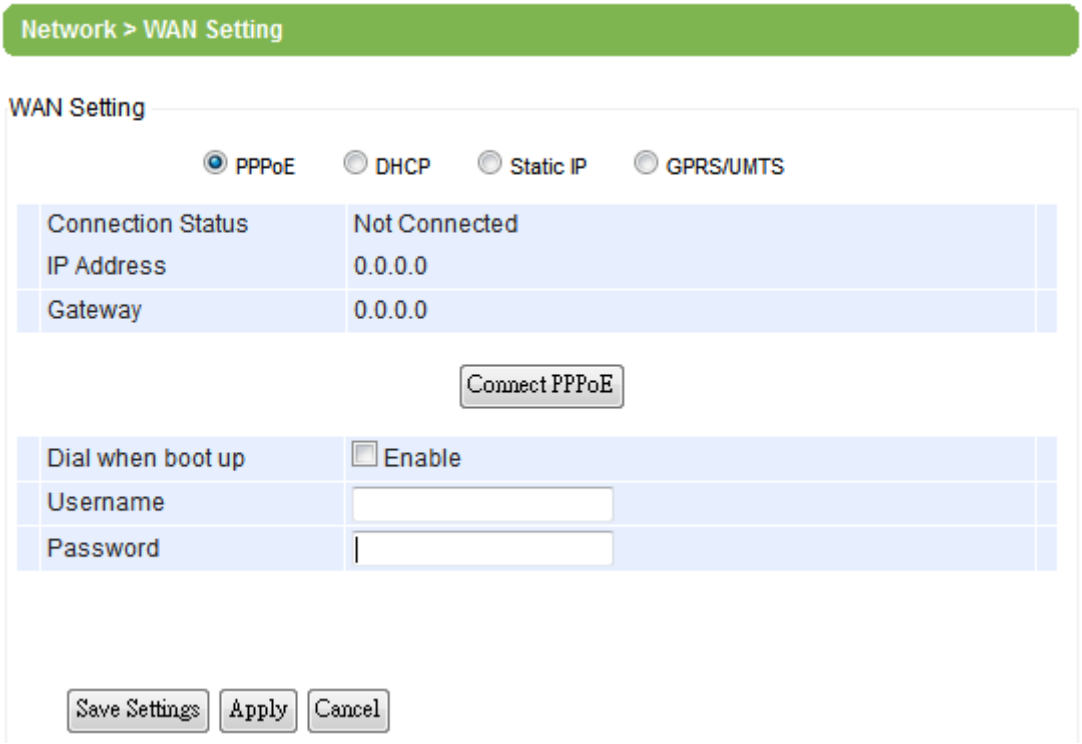


Figure 4.17

4.4.4 Virtual Server (Regular AP Gateway Mode)

Virtual Server's function is to modify the IP address information in IP packet headers while in transit across a traffic routing device. Enabling this function allows the devices using a private IP address in the LAN to be accessible from the Internet through IS150. You can set the ports to be translated.

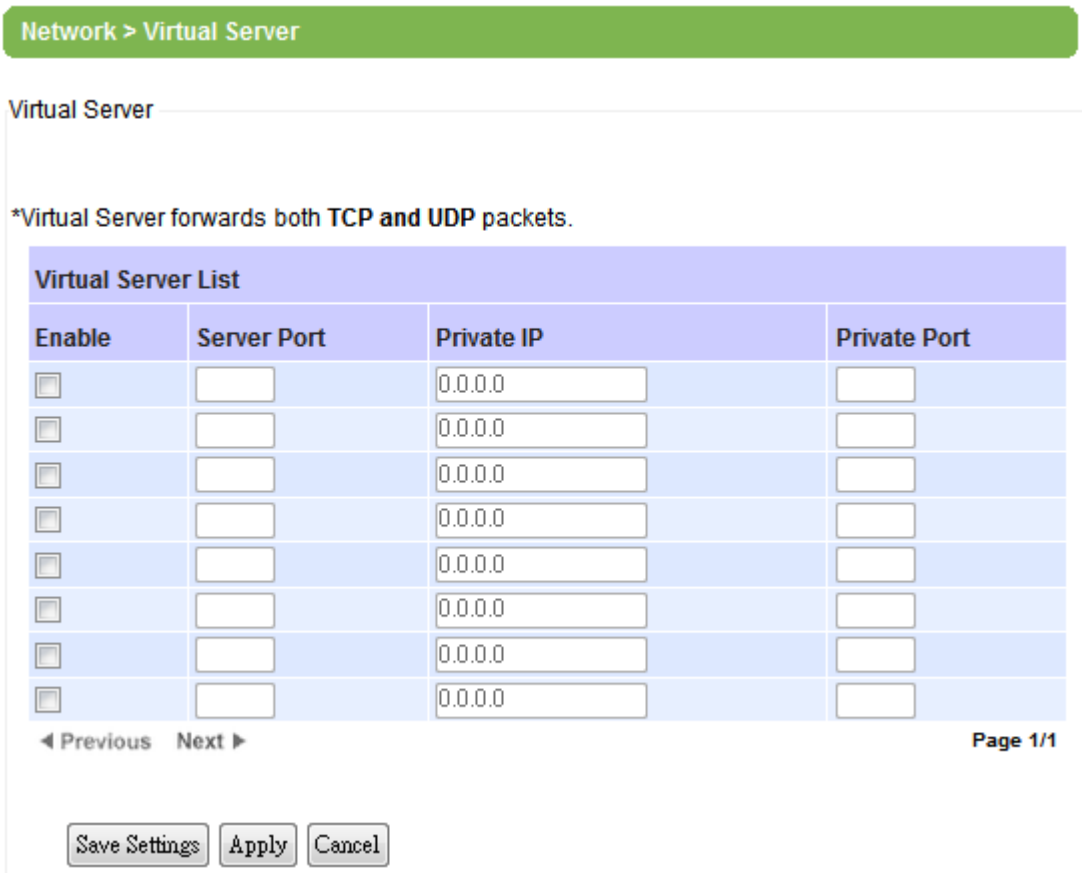


Figure 4.18

4.4.5 SNMP Settings

The SNMP is used by network management software to monitor devices in a network to retrieve network status information and to configure network parameters. The SNMP Settings shows the configuration of this device so it can be viewed or edited by third-party SNMP software as shown below, Figure 4.19.

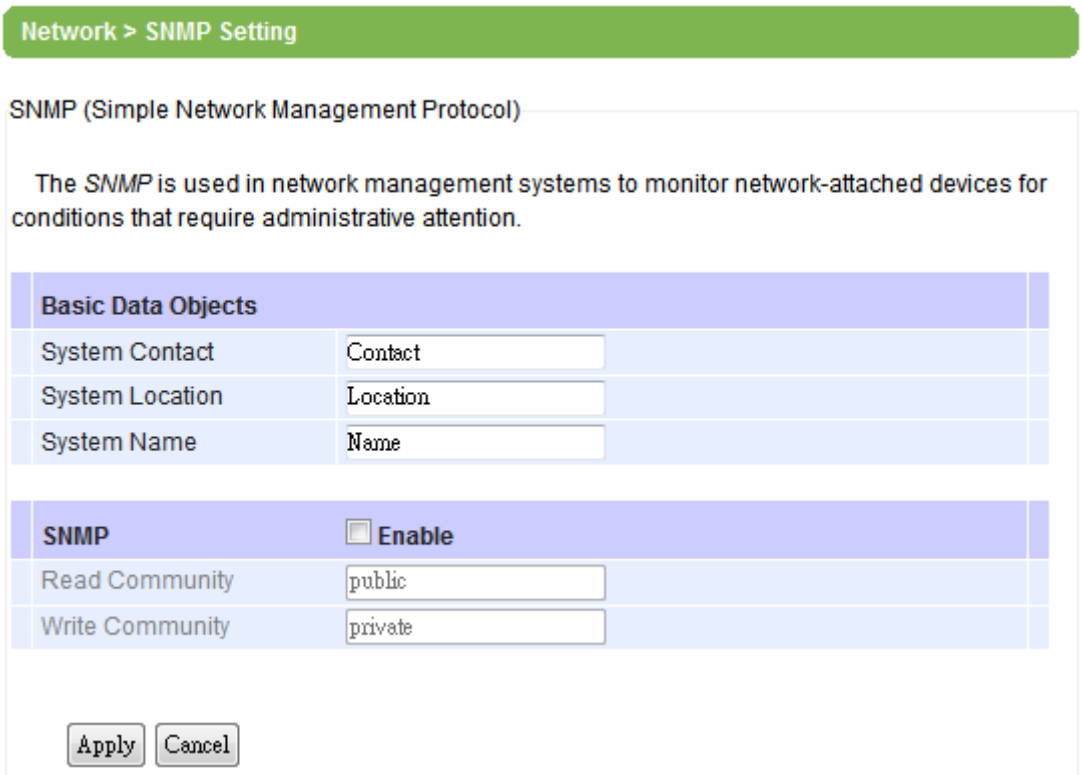


Figure 4.19

IS150 provides two SNMP fields, which are **"System Contact",** usually used to specify the device's contact information in case of emergency; and **"System Location",** usually used to specify the device location.

If you wish to make the device information available for public viewing/editing, **Enable** the SNMP function. Fill in the passphrase for the **"Read Community"**, the group that is allowed to read the device information and fill in the passphrase for the **"Write Community"**, the group that is allowed to read/modify the device information. By default IS150 comes in **public** for **Read Community** and **private** for **Write Community**.

4.4.6 DHCP Server (Regular AP Gateway Mode)

If there is no workstation or server to act as the DHCP Server and assign IP addresses to each client automatically, IS150 can serve as the DHCP Server to statically or dynamically assign an IP address to any network device. To enable such functionality, check **Enabled** to enable the DHCP Server in IS150**;** proceed then to fill in the **IP Address Range** including the **"From IP Address"** and **"To IP Address"**, fill in the IP address' **Netmask** (or **Subnet Mask**). **"Lease Time"** is the duration in minutes that an assigned IP Address will belong to that device; once expired, the IP address will be recycled. A maximum of 21600 minutes is set by default.

You can also assign a static IP address to a network device, meaning that the network device would always get the same Static IP Address from the DHCP server. To statically assign an IP address, check on the small box in front of each line, and then fill in the **Host Name** and/or the **MAC Address** that you want to assign a static **IP Address** to. When DHCP is enabled, up to 32 different static IP/MAC can be set, Figure 4.20.

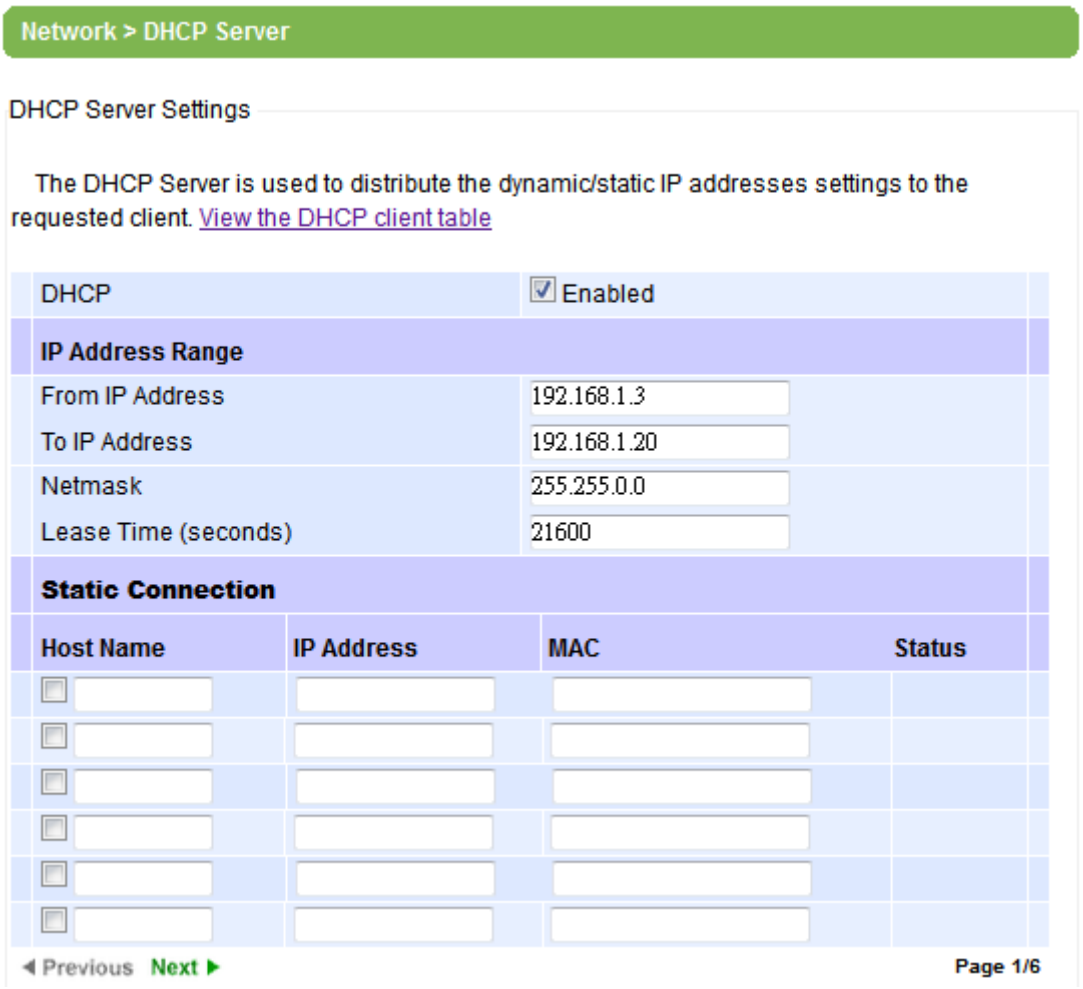


Figure 4.20

For a look at the current DHCP client table, just click where it says **"View the DHCP client table"**, if no clients are present there would be a message specifying so Figure 4.21 .

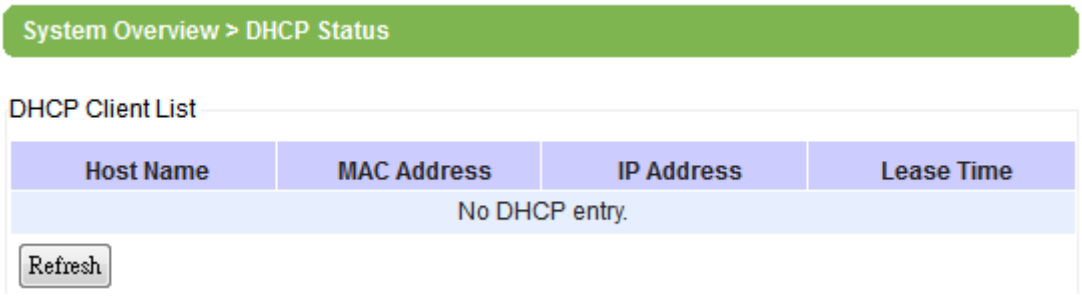


Figure 4.21

4.5 Wireless Settings

Wireless Settings includes the basic Wi-Fi settings and wireless security. There are however, some concepts to be mentioned before going one step forward on the wireless settings. As you know, 802.11 is a set of standards for WLAN communication at the 2.4, 3.6 and 5 GHz frequencies. The IS150 works only with the 2.4 and 5 GHz range, it follows the below mentioned standards:

- **802.11a;** (also known as 802.11a-1999), is a 54 Mbps (around 20 Mbps net throughput), 5 GHz signaling standard; since 2.4 GHz is used by a big number of different devices interference here is less than in 802.11b. However, signals will not penetrate as much as 802.11b because they are absorbed more readily by walls and other solid objects (when on a single path), but not when use in multi-path environments i.e., indoors, office.
- **802.11b;** the first of the standards to be created; an 11 Mbps (4~5 Mbps net throughput), 2.4 GHz signaling standard. Although it performs much better than traditional dial-up networking, its performance is still significantly less than 802.11a and other, newer standards.
- **802.11g;** very similar to 802.11b, the main difference being that it is done in a maximum raw data rate of 54 Mbps (20 Mbps net throughput), at the same 2.4 GHz bandwidth
- **802.11n;** more resistant to signal interference from outside sources. Improves the amount of bandwidth supported by using multiple wireless signals and antennas (MMO technology) instead of one. Net throughput on a 2x2 solution is about 100 Mbps on our models.

4.5.1 Secure Wireless Wi-Fi Network

When Wi-Fi is enabled, we recommend using WPA2-PSK with AES as a minimum when securing your network; also remember to set it at 802.11n for a full speed performance. For more information

on this and more please read **Security Settings**.

4.5.2 Basic Settings (Regular AP Gateway)

To set up a wireless network in the Regular AP Gateway mode, several parameters are needed as shown in Figure 4.22. Link Speed can be optimized up to 300 Mbps by choosing 802.11 b/g/n or 802.11a/n; again, remember that 2.4 GHz frequency is easily interfered by other devices that operate in the same region (namely, Bluetooth, Zigbee, Microwave, etc.) so it is better to choose the 802.11a/n which operates in the 5 GHz when your network allows it. Below there is a table which shows the default wireless **Basic Settings** for the device, Table 4.2.

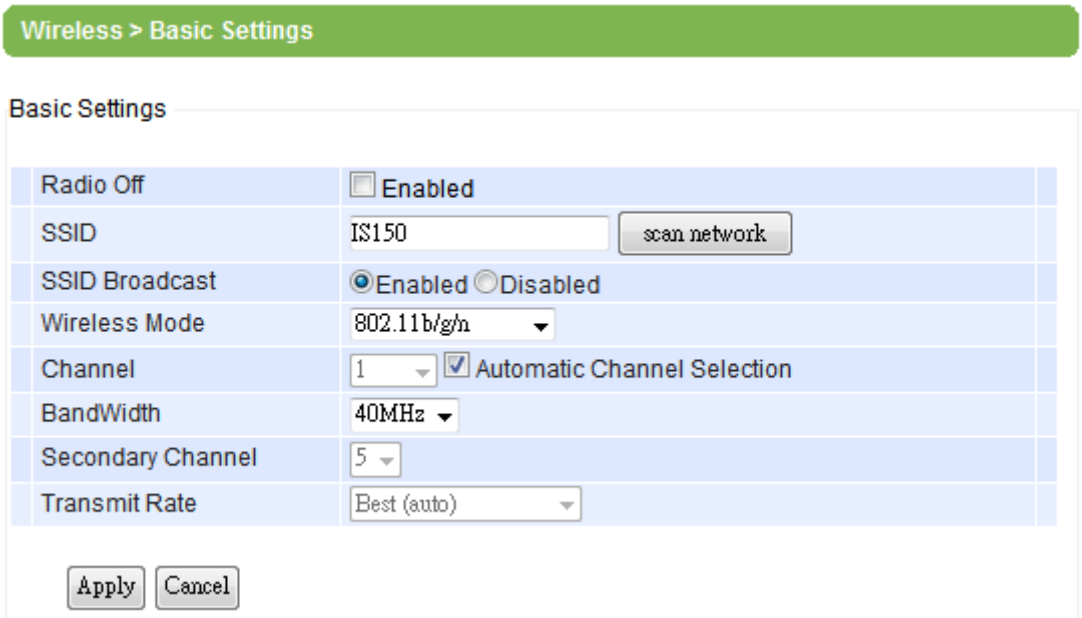


Figure 4.22

Table 4.2

Caption	Default
Radio Off	Disabled
SSID	IS150
SSID Broadcast	Enabled
Wireless Mode	802.11b/g
Channel	1 (Automatic Channel Selection box checked)
Bandwidth	40 MHz
Secondary Channel	5
Transmit Rate	Best (auto)

The basic settings are explained in detail below:

- **Radio Off:** When enabled, wireless radio would turn off completely.
- **SSID:** specifies the device's wireless network name that other wireless devices should use in order to associate with this AP. There is a **"Scan Network"** button to the right of the empty box. You can use the **"Scan network"** function to learn about the different SSIDs and channel numbers in the device's surroundings, please be patient as this process might take as long as 10 seconds as shown in Figure 4.23. Once it has finished scanning, names and basic properties of neighboring networks will be shown as in Figure 4.24. When no neighbors have been found the answer is as follows Figure 4.25. Keep in mind that the SSID should be unique unless wireless roaming is required.

Figure 4.23

SSID	MAC Address	T	Mode	Channel	Authentication	Encryption	Mbps	Signal%
banmu02	8C:4D:EA:00:14:93	Infra	b/g	6	WPA2-PSK	TKIP	54	1
sw5502-test	2A:7D:D8:0B:4E:BD	Adhoc	b/g/n	1,5	OPEN	NONE	144	3

T is Topology (Infra = Infrastructure, Adhoc)
Channel is listed as Primary Channel, Secondary Channel

Refresh Close

Figure 4.24

SSID	MAC Address	T	Mode	Channel	Authentication	Encryption	Mbps	Signal%
There is no wirelesss network detected.								

T is Topology (Infra = Infrastructure, Adhoc)
Channel is listed as Primary Channel, Secondary Channel

Refresh Close

Figure 4.25

- **SSID Broadcast:** allow any wireless client to search for this access point presence, it is enabled by default. When the **SSID Broadcast** is disabled, wireless clients need to manually input the SSID in their wireless client configuration, increasing network security to prevent an access from unsolicited clients.
- **Wireless Mode:** The modes are separated into two parts by different colors. The modes colored in green denotes the modes that runs on the 2.4 GHz frequency and the modes colored in red denotes the modes that runs on the 5 GHz frequency. Please note that the 2.4 GHz frequency is very crowded and usually does not reflect the real performance of the device, please consider using the 5 GHz frequency when possible.
- **Channel**: Select **"Automatic Channel Select"** to let the device automatically assign the best available channel number. When setting the channels manually, bear in mind that channels 1, 6,

and 11 are the non-overlapping channels for 2.4 GHz, Figure 4.26. Again, you can use **"Scan network"** to see which channels are already occupied.

- **Bandwidth**: when 40 MHz is used, IS150 will double the channel width to 40 MHz as compared to the standard 20 MHz to transmit its data; this is not recommended for 802.11b/g/n since it will leave only one non-overlapping channel for other APs. HT40 (40 MHz), is recommended for 802.11a/n because it offers a wider frequency range and it is easier for IS150 to find empty channels as well.

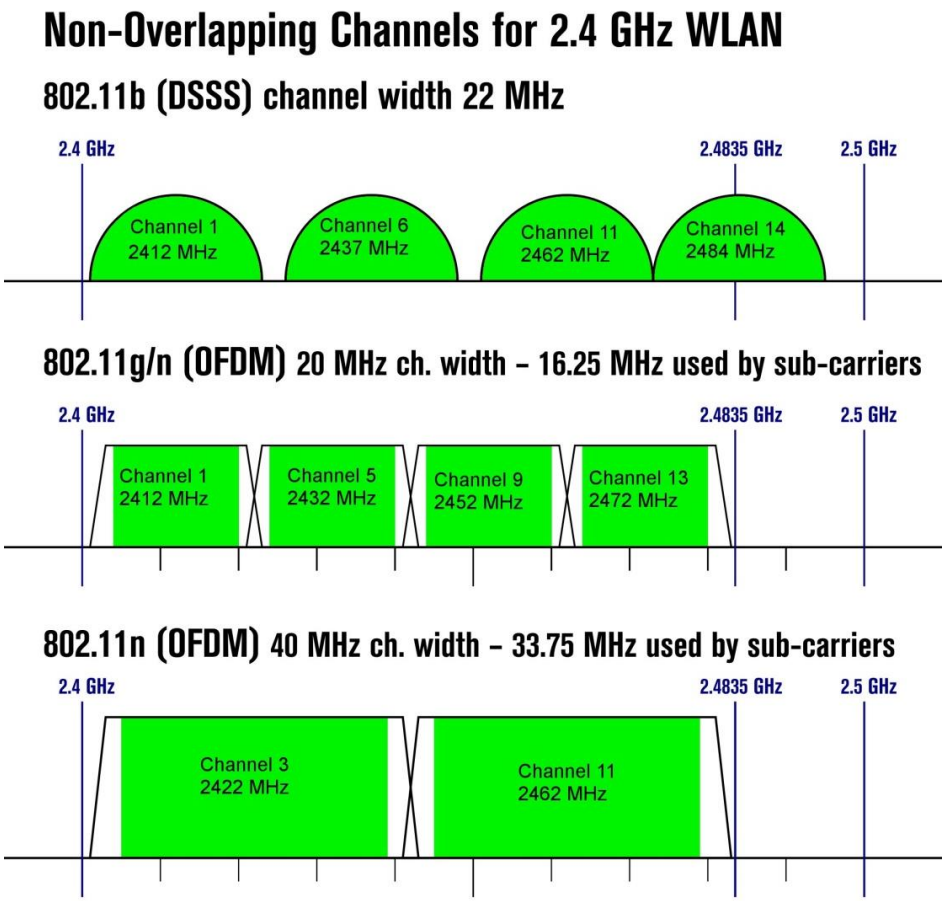


Figure 4.26

- **Secondary Channel:** the second channel that IS150 uses when the 40 MHz bandwidth is enabled, a better description is given on Table 4.3 and Table 4.4.

Table 4.3

2.4 GHz Primary channel	20 MHz	40MHz upper			40 MHz lower		
	Blocks	2nd ch.	Center	Blocks	2nd ch.	Center	Blocks
1	1-3	5	3	1-7	Not Available		
2	1-4	6	4	1-8			
3	1-5	7	5	1-9			
4	2-6	8	6	2-10			
5	3-7	9	7	3-11	1	3	1-7
6	4-8	10	8	4-12	2	4	1-8
7	5-9	11	9	5-13	3	5	1-9
8	6-10	12	10	6-13	4	6	2-10
9	7-11	13	11	7-13	5	7	3-11
10	8-12	Not Available			6	8	4-12
11	9-13				7	9	5-13
12	10-13				8	10	6-13
13	11-13				9	11	7-13

Table 4.4

5 GHz Primary channel	40MHz upper	40 MHz lower
	2nd channel	2nd channel
36	40	-
40	-	36
44	48	-
48	-	44
60	64	-
64	-	60
149	153	-
153	-	149
157	161	-
161	-	157

- **Transmit Rate:** a maximum data transmission of 300 Mbps is supported. This option is disabled,

so IS150 will use the best possible rate.

Table 4.5

MCS index	Spatial streams	Modulation type	Data rate (Mbit/sec)			
			20 MHz channel		40 MHz channel	
			800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	6.50	7.20	13.50	15.00
1	1	QPSK	13.00	14.40	27.00	30.00
2	1	QPSK	19.50	21.70	40.50	45.00
3	1	16-QAM	26.00	28.90	54.00	60.00
4	1	16-QAM	39.00	43.30	81.00	90.00
5	1	64-QAM	52.00	57.80	108.00	120.00
6	1	64-QAM	58.50	65.00	121.50	135.00
7	1	64-QAM	65.00	72.20	135.00	150.00
8	2	BPSK	13.00	14.40	27.00	30.00
9	2	QPSK	26.00	28.90	54.00	60.00
10	2	QPSK	39.00	43.30	81.00	90.00
11	2	16-QAM	52.00	57.80	108.00	120.00
12	2	16-QAM	78.00	86.70	162.00	180.00
13	2	64-QAM	104.00	115.60	216.00	240.00
14	2	64-QAM	117.00	130.00	243.00	270.00
15	2	64-QAM	130.00	144.40	270.00	300.00

4.5.3 Mobile Station (AP Client)

To set up a wireless network in the AP Client mode, several parameters are needed as shown in Figure 4.27. Below there is a table which shows default **Mobile Station** Settings for the device, Table 4.6.

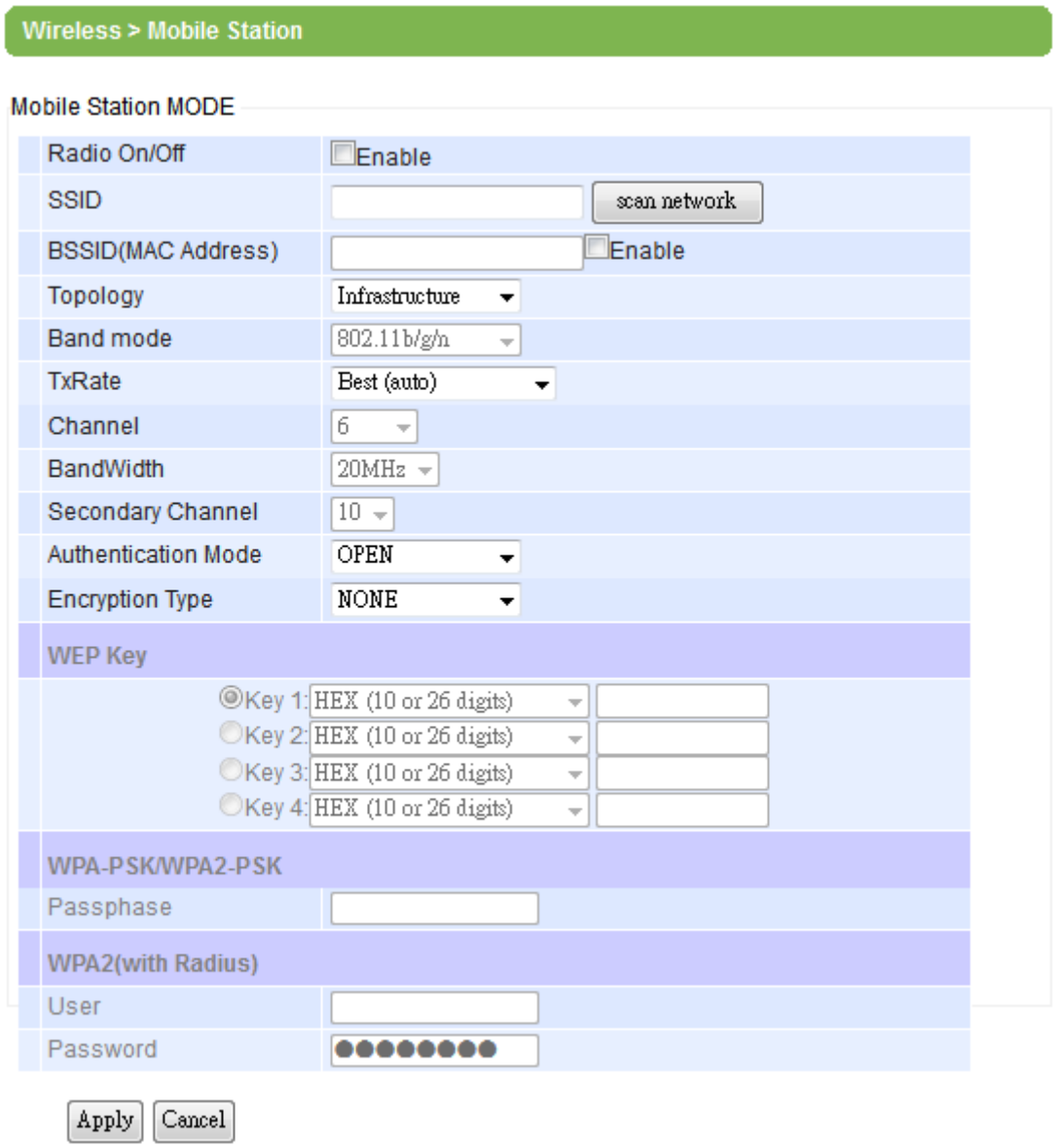
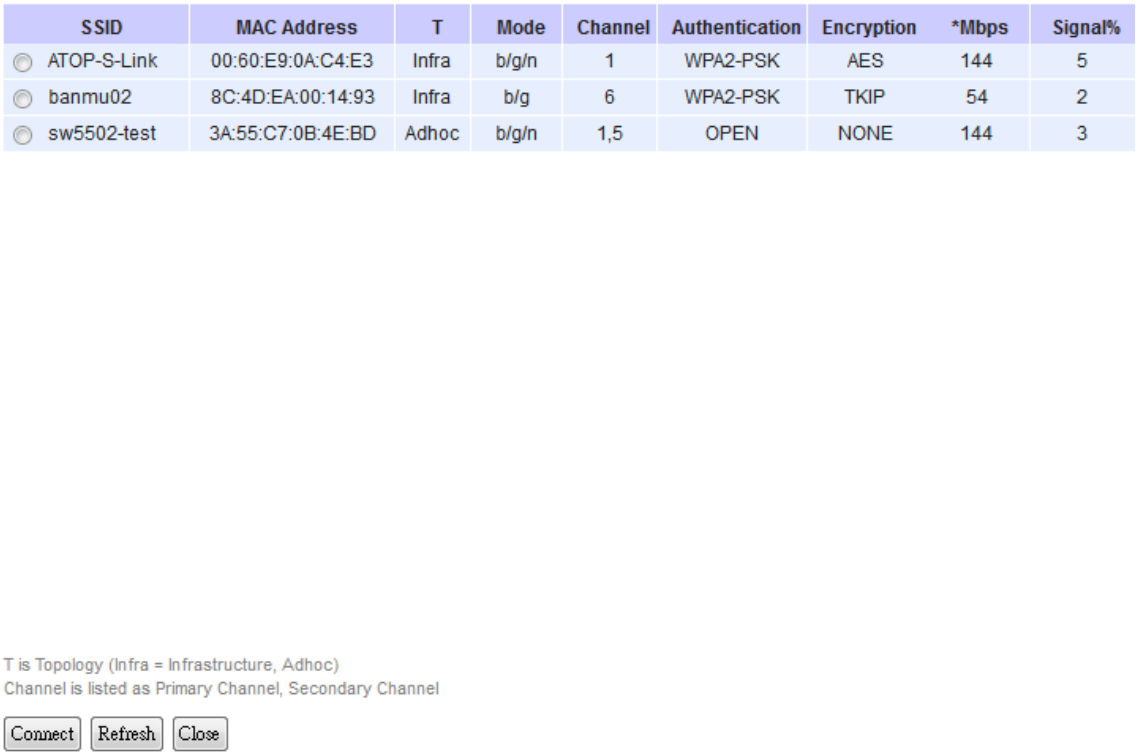


Figure 4.27

Table 4.6

Caption	Default
Radio Off	Disabled
SSID	Null (Any)
BSSID (MAC Address)	Disabled
Topology	Infrastructure
Band Mode	Automatic Detection
Tx Rate (transmission rate)	Best (auto)
Channel	Automatic Detection
Bandwidth	Automatic Detection
Secondary Channel	Automatic Detection
Authentication Mode	OPEN
Encryption Type	NONE

- **SSID:** specifies the SSID (network name) that IS150 should connect to wirelessly. There is a **"Scan Network"** button to the right of the empty box, this button makes it possible to look for available wireless networks to attach to. Once clicked, it will start scanning and prompt a window, please be patient as this process might take as long as 10 seconds as shown in Figure 4.23. Once it has finished scanning, select the AP that you wants to connect to as in Figure 4.27. When no AP is found, please adjust the position of IS150 or the angel of its antenna to improve the signal quality.



SSID	MAC Address	T	Mode	Channel	Authentication	Encryption	*Mbps	Signal%
ATOP-S-Link	00:60:E9:0A:C4:E3	Infra	b/g/n	1	WPA2-PSK	AES	144	5
banmu02	8C:4D:EA:00:14:93	Infra	b/g	6	WPA2-PSK	TKIP	54	2
sw5502-test	3A:55:C7:0B:4E:BD	Adhoc	b/g/n	1,5	OPEN	NONE	144	3

Figure 4.28

- **BSSID:** this refers to the Access Point MAC address on which the IS150 should connect to. Enabling this option will lock IS150 to that Access Point, so IS150 would not roam to another Access Point with the same SSID.
- **Topology:** Infrastructure (for connecting to an Access Point) or Adhoc (for connecting to a wireless client). Note that **Adhoc** mode is unavailable when the **Wireless Profiles** is enabled.
- **Band Mode:** 802.11b, 802.11b/g, 802.11b/g/n, 802.11a, and 802.11a/n are available. We suggest leaving this option to **Auto** for IS150 to sense the best available mode.
- **Tx Rate:** different rates are available, it is suggested to leave this to **Best (auto).** This option is disabled when the band mode is set to Auto.
- **Channel:** the available channels would depend on the band mode and the regulatory domain selected in the Wireless Advanced Settings. This option is disabled when the band mode is set to Auto.
- **Bandwidth:** select between 20 MHz or 40 MHz; the latter fills a larger spectrum, hence it provides a better throughput if it Is allowed by the Access Point. It is not recommended to use 40 MHz@2.4 GHz (802.11b/g/n).
- **Secondary Channel:** the second channel that IS150 uses when the 40 MHz bandwidth is enabled.
- **Authentication Mode:** Select between OPEN, WPA-PSK, WPA2-PSK, WPA2 (PEAP),

WPA2(EAP-TLS), and WPA2(EAP-TTLS).

- **Encryption Type:** Select between WEP, TKIP and AES. Please be aware that WEP and TKIP are not supported by the 802.11n standard, so the wireless link speed would be limited to 54Mbps.
- **WEP Key:** Enable when Authentication is set to OPEN and Encryption is set to WEP. Up to 4 different hexadecimal or ASCII keys can be entered in this section.
- **WPA-PSK/WPA2-PSK Passphrase:** Enable when Authentication is set to WPA-PSK or WPA2-PSK. It can be between 8 and 63 characters long.
- **WPA2 (with RADIUS):** Depending on the Authentication Mode selected, different fields would be enabled. **WPA2 (PEAP)** would require you to provide the user, password, and the certificates. **WPA2 (EAP-TLS)** would require you to provide the certificates and private key password. **WPA2 (EAP-TTLS)** would require you to provide the user, password, and the certificates. Please note that only *.pem certificates are supported.

4.5.4 Security Settings (Regular AP Gateway Mode)

These settings provide an overall network security (according to the user's needs), by default Wireless Security is Disabled, Figure 4.29. Each AP (SSID) can have its own wireless security. For example, you can create a temporary SSID with OPEN security for guest access. Note that WEP will not be available if you have enabled more than one AP (SSID).

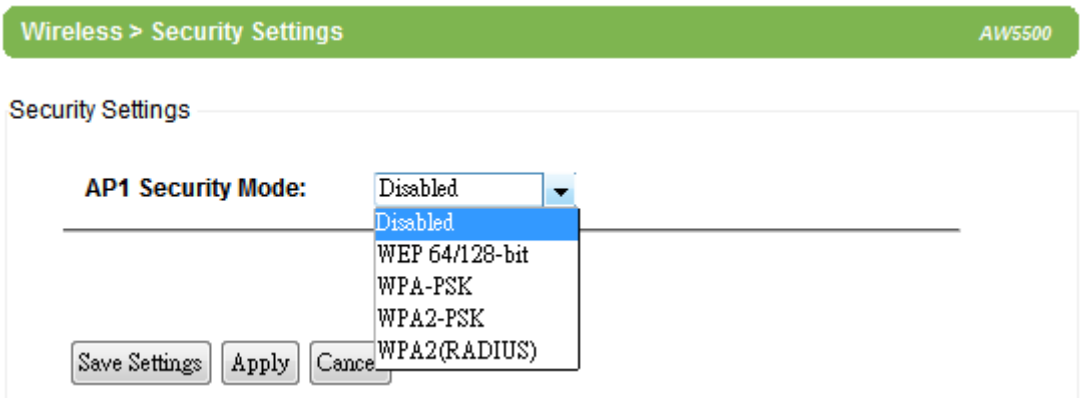


Figure 4.29

A number of Security Settings are available for you:

- **WEP 64/128-bit Hex:** stands for **W**ired **E**quivalent **P**rivacy. Which is a moderately weak security algorithm, and although it implies security in a wired connection, it is weaker than **WPA** protocols. It is not recommended unless a really large network is being administered. Up to 4

different hexadecimal or ASCII keys can be entered in this section, Figure 4.30.

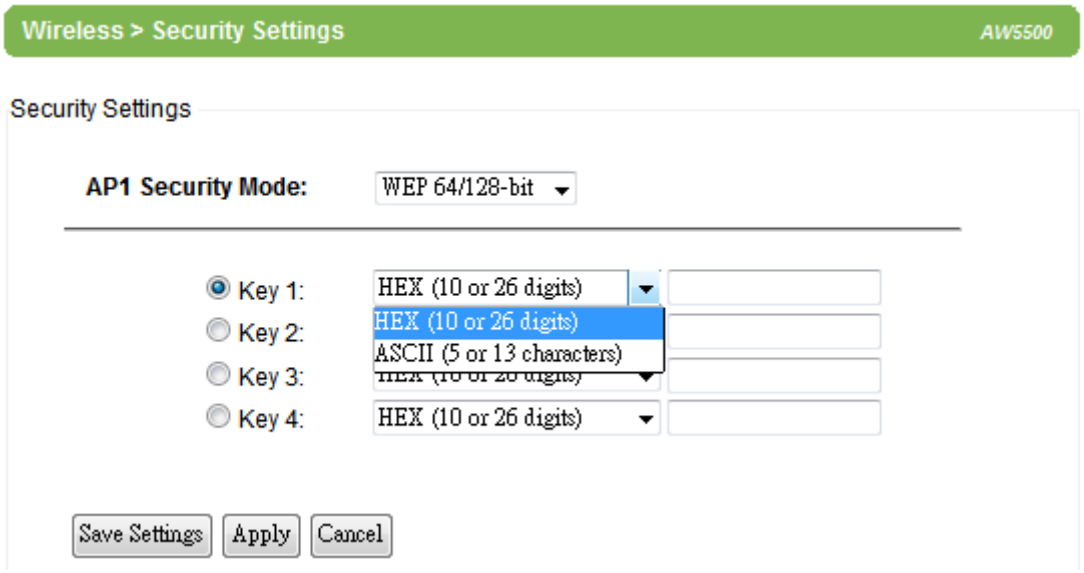


Figure 4.30

- **WPA-PSK:** stands for **W**i-Fi **P**rotected **A**ccess. Uses a passphrase generated and entered by the user; this passphrase can be between 8 and 63 characters long. We strongly recommend not to take a passphrase already in use within the network (nor use a variation of personal information publicly available), since this can compromise network's security, Figure 4.31.

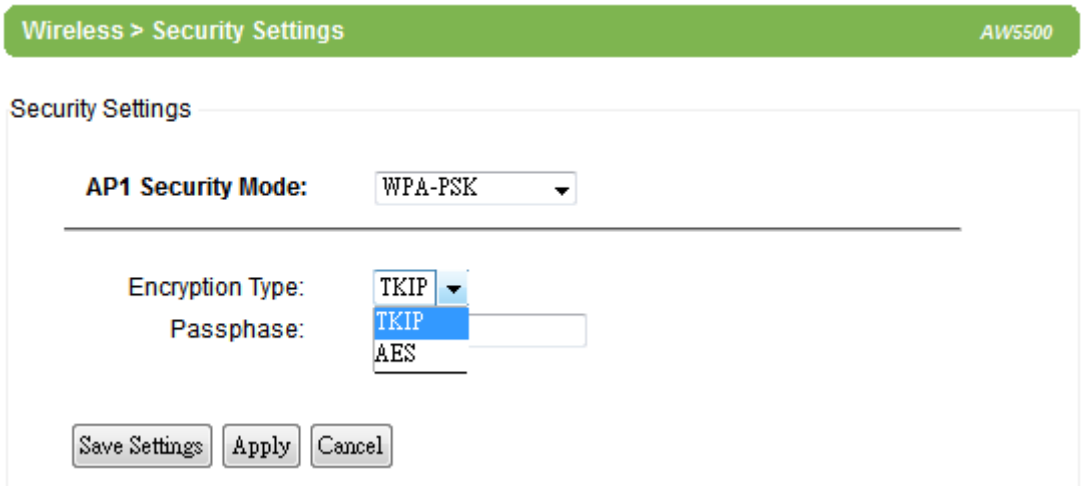


Figure 4.31

- **WPA2-PSK:** stands for **W**i-Fi **P**rotected **A**ccess **II**. This is a highly recommended setting for the average user. You can select the encryption mode tone of the following: TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol), or AES (**A**dvanced **E**ncryption **St**andard). Less prone to be hacked than the above one, Figure 4.32.

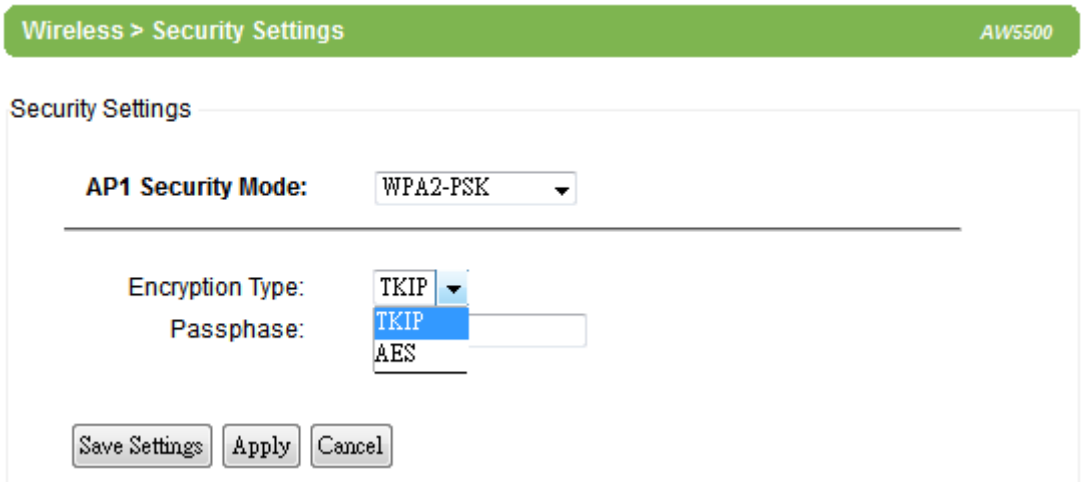


Figure 4.32

- **WPA2 (RADIUS):** designed for enterprise networks, it requires a RADIUS (**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice), authentication server. Although possessing a more complicated setup, security is optimized since passwords are not transmitted between the NAS (**N**etwork **A**uthentication **S**erver) and RADIUS, Figure 4.33.

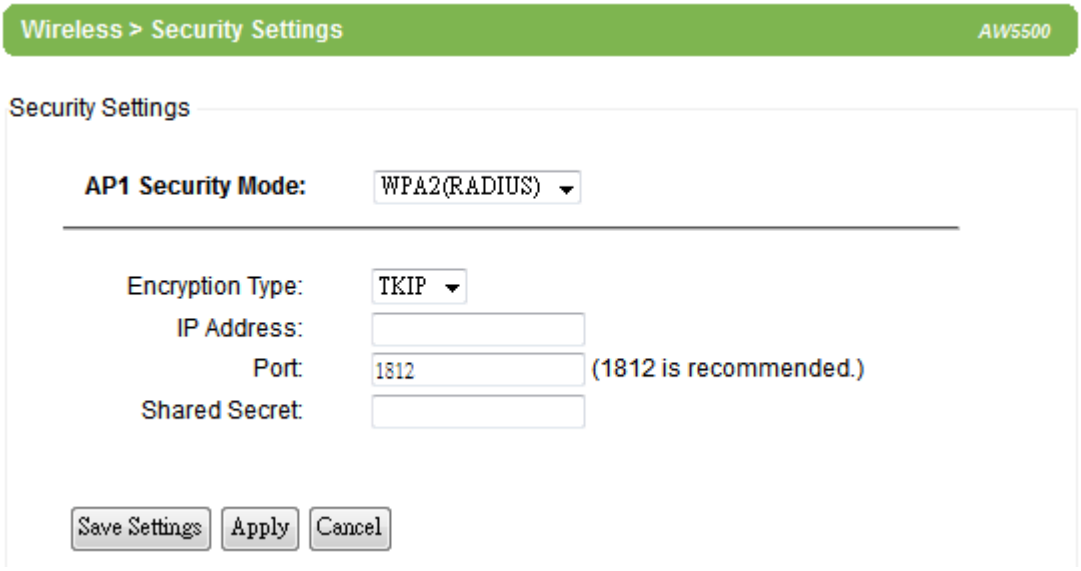


Figure 4.33

- **Disabled:** no security settings are being used in the current device (comes as factory default), Figure 4.34. **This option is highly discouraged since authentication as well as encryption is not performed in this mode.**

Figure 4.34

4.5.5 Advanced Settings

Provide details on wireless parameters for performance tuning. Changes in this section may affect overall performance, so caution is recommended, if you are not clear of what you are doing please refrain from altering them, Figure 4.35.

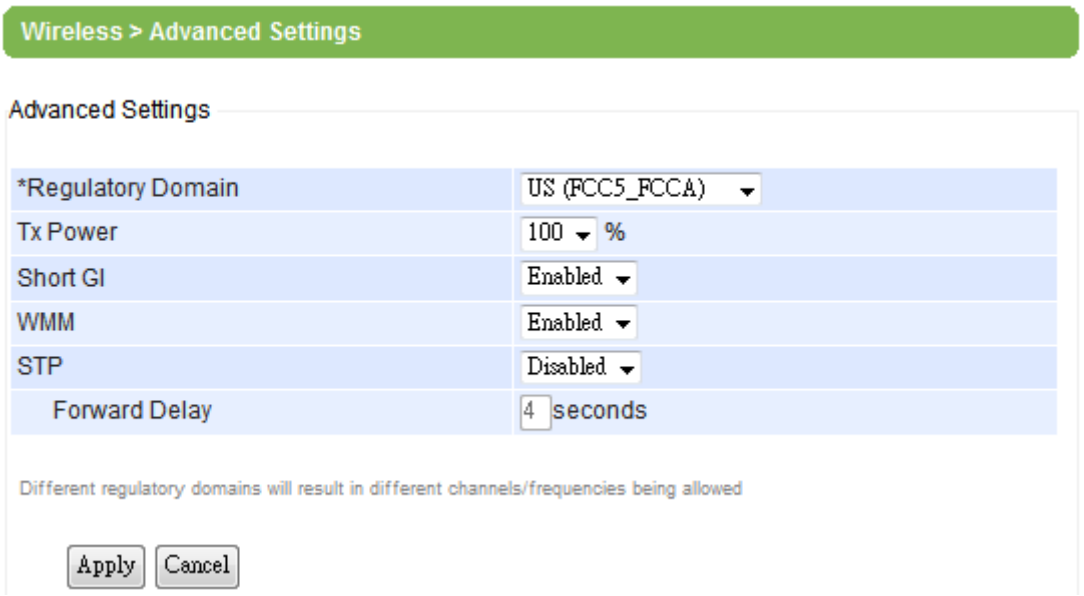


Figure 4.35

- **Regulatory Domain:** Change this settings according to the country where is the device is installed, which are CN (China), EU (European Union), TW (Taiwan), and US (United States).

- **TX Power** is IS150's **T**ransmission **P**ower. The transmission power can be reduced to prevent wireless interference to other wireless networks.
- **Short GI** is recommended to leave it as enabled to maximize the throughput.
- **WMM** or **W**ireless **M**ultimedia Extension, which is recommended to leave as enabled in order to comply with 802.11n standards and achieve link speeds higher than 54 Mbps.
- **STP** or Spanning Tree Protocol, please enable this option if STP is enabled in your network to prevent network loops. When disabled, IS150 will not forward STP BPDUs. **Forward Delay** time in which the interface takes to converge from blocking stage to forwarding state. This option only shows in the **AP Client** mode.

4.6 Input / Output

Determine whether the onboard DO1 and DO2 (relay out) should be triggered on or not.

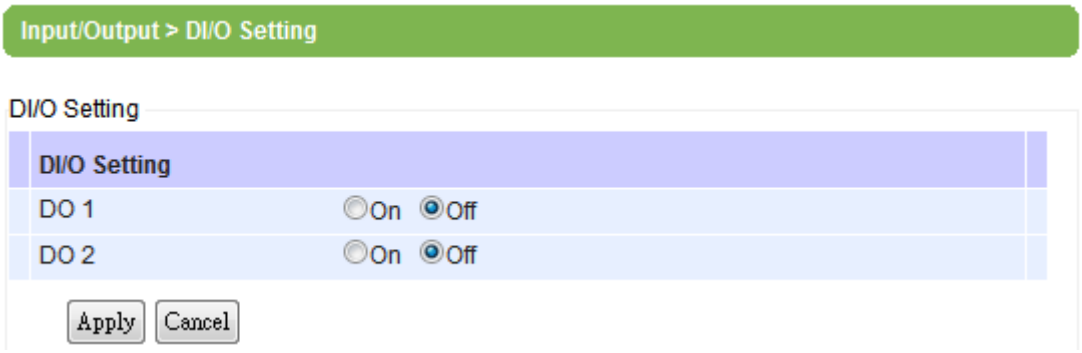


Figure 4.36

4.7 System Setting

The following section describes some critical settings for the IS150; take care when changing the values here as they will greatly influence your network performance.

4.7.1 Firmware Upgrade

Updated firmware is provided by our company from time to time to fix bugs and optimize performance. It is very important that the device must **NOT be turned off or powered off during the firmware upgrading, (please be patient as this whole process might take up to 8 minutes)**. Before upgrading the firmware, please make sure that the device has a reliable power source that will not be powered off or restarted during the upgrading process. To upgrade a new firmware, once downloaded, copy the new firmware file to your computer, and then click **"Browse"** to find the new firmware file, then click **"Upload".** The program will show the upload status, please wait until the uploading process is finished; the device will then proceed to restart itself (Figure 4.37).

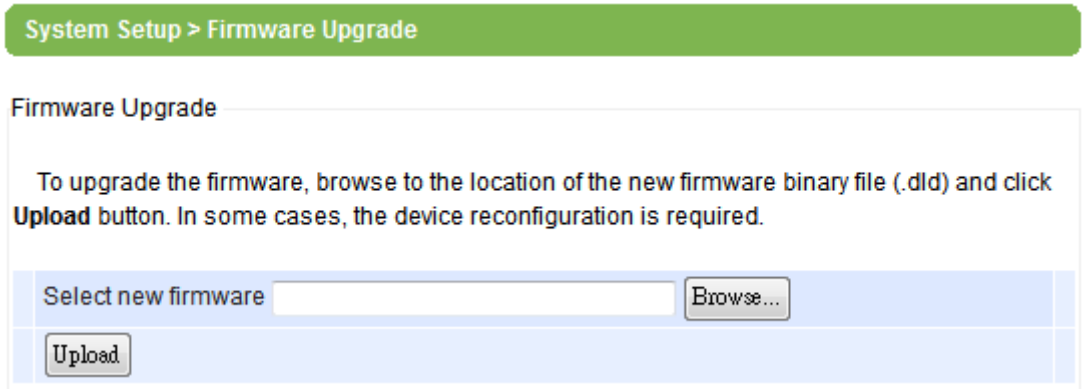

System Setup > Firmware Upgrade
Firmware Upgrade
To upgrade the firmware, browse to the location of the new firmware binary file (.dld) and click Upload button. In some cases, the device reconfiguration is required.
Select new firmware
Browse...
Upload

Figure 4.37

4.7.2 Time

Date and time can be set manually, or using **N**etwork **T**ime **P**rotocol (NTP) to automatically synchronizes with a Time Server. For auto-synching check the box below **NTP Server Settings "Obtain date/time automatically"** proceeding then to fill the IP address or host name for it if a hostname is entered, the DNS server must be configured properly; a Time Zone can be selected as well, Figure 4.38.

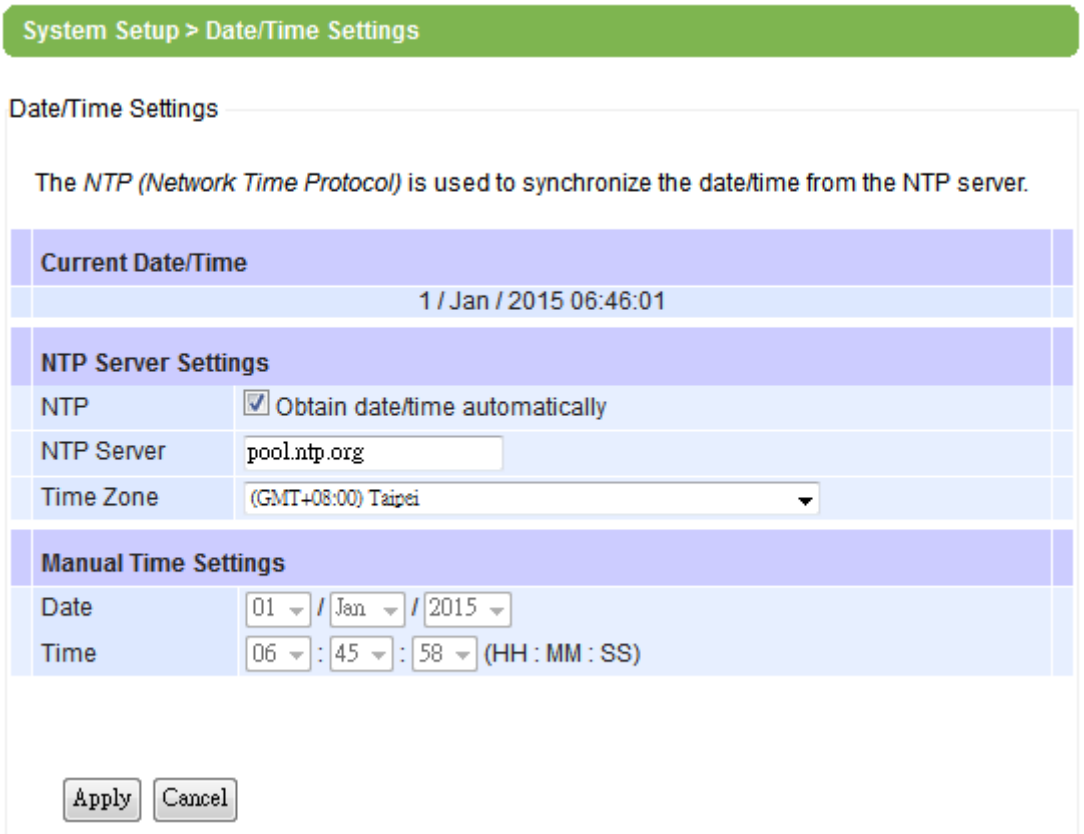


Figure 4.38

4.7.3 Password

The IS150 allows User and password management, the user's default is as "admin" and the password will be in blank as default. The Device name entry can be changed as well; to set/change their value just follows the steps filling in the corresponding blanks and choose **Apply** in the end, Figure 4.39.

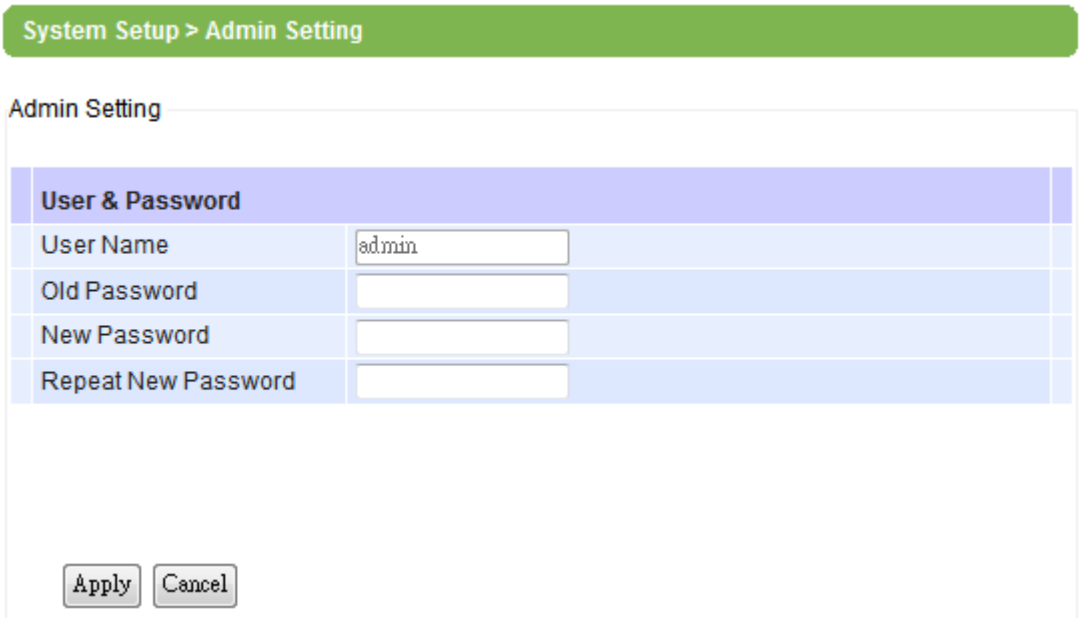


Figure 4.39

4.7.4 Restore to Default

To restore the device to its factory default settings, click on “Reboot”. You will lose all your configurations by doing this.

Also, you could use the button located inside the device, close to the LAN2. Hold it long enough until the device produce a long beep, release the button and wait for the device to restart.

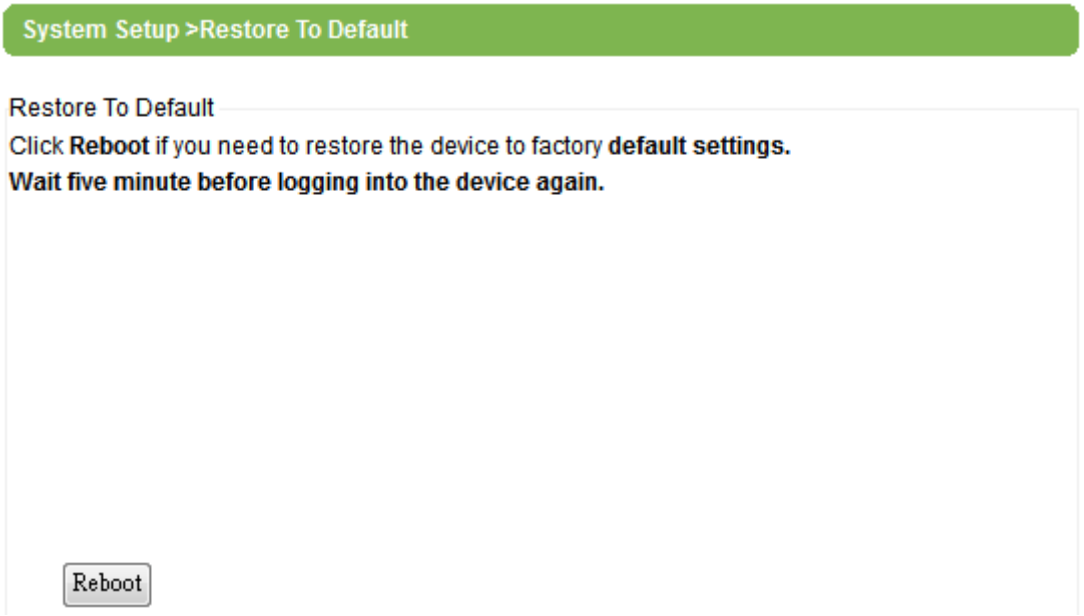

System Setup >Restore To Default
Restore To Default
Click Reboot if you need to restore the device to factory default settings.
Wait five minute before logging into the device again.
Reboot

Figure 4.40

4.7.5 Reboot

To manually reboot the device, you may click on “Warm Start”, after which the device will restart.

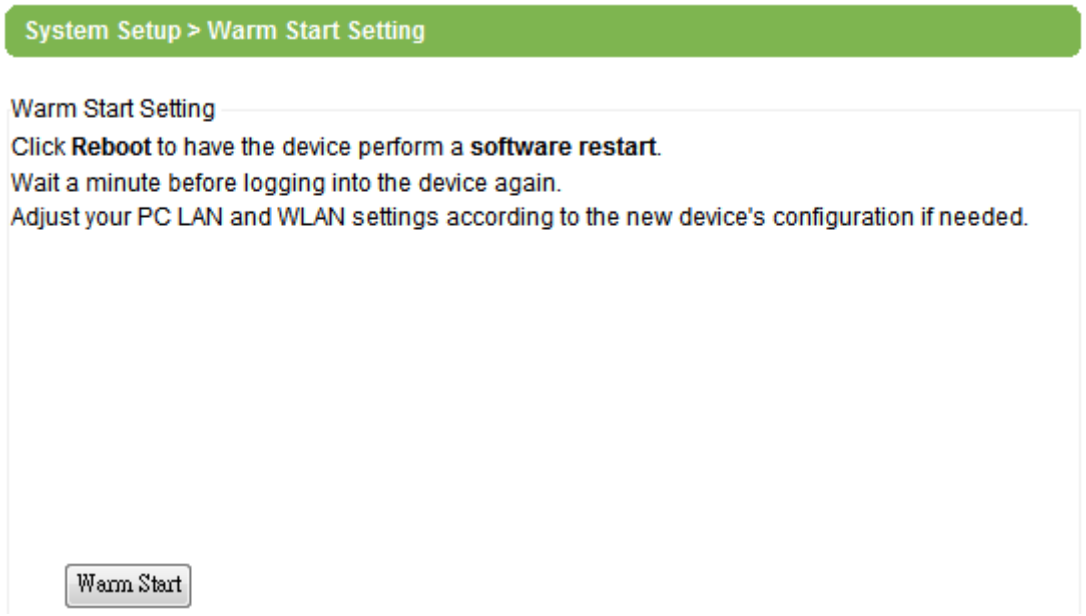

System Setup > Warm Start Setting
Warm Start Setting
Click Reboot to have the device perform a software restart.
Wait a minute before logging into the device again.
Adjust your PC LAN and WLAN settings according to the new device's configuration if needed.
Warm Start

Figure 4.41

4.8 Logout

Click on logout to terminate this session and prevent unauthenticated people from accessing the Web UI using this browser.

5 WAN Configuration

5.1 PPPoE

Often used when there is an xDSL connection provided by your Internet Service Provider (ISP). Enter the **Username** and **Password** provided by your ISP in the blank fields (Figure 5.6). If you want IS150 to connect to the Internet automatically when it boots up, enable "**Dial when boot up**."

Note: IS150 uses Port 2 (the upper port) as the WAN port.

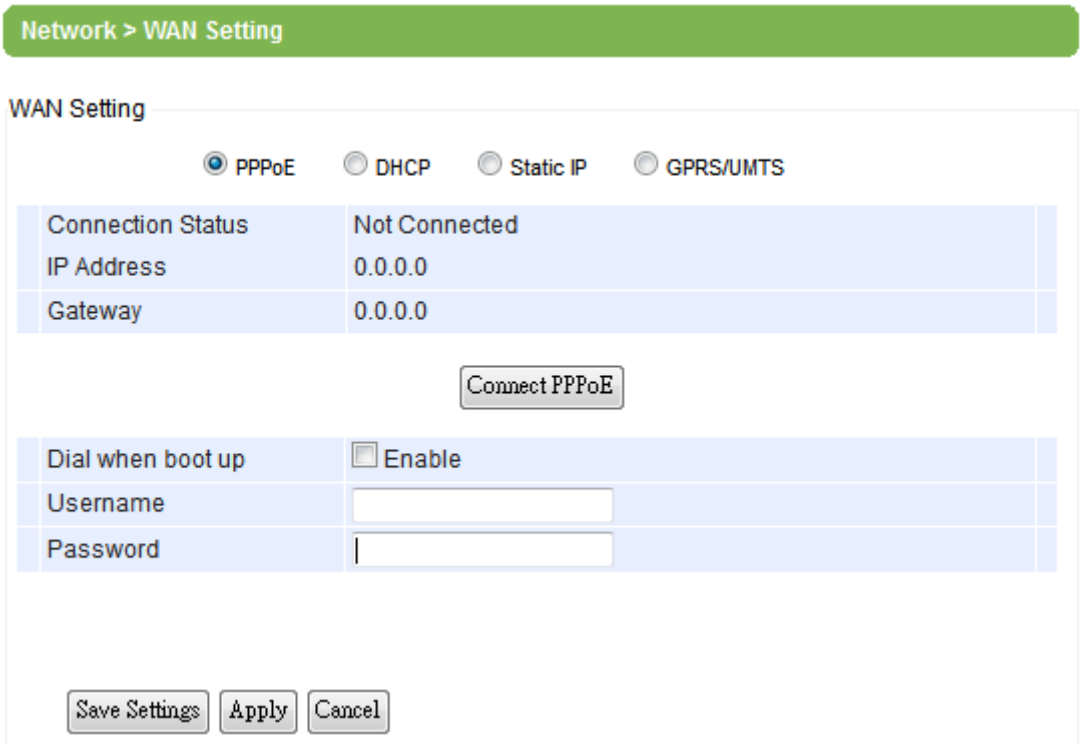


Figure 5.1

Double check your configuration by clicking "**Connect PPPoE**." If **PPPoE** has connected successfully, the connection status will become **Connected** with an **IP** and **Gateway** obtained from the ISP as in Figure 5.2.

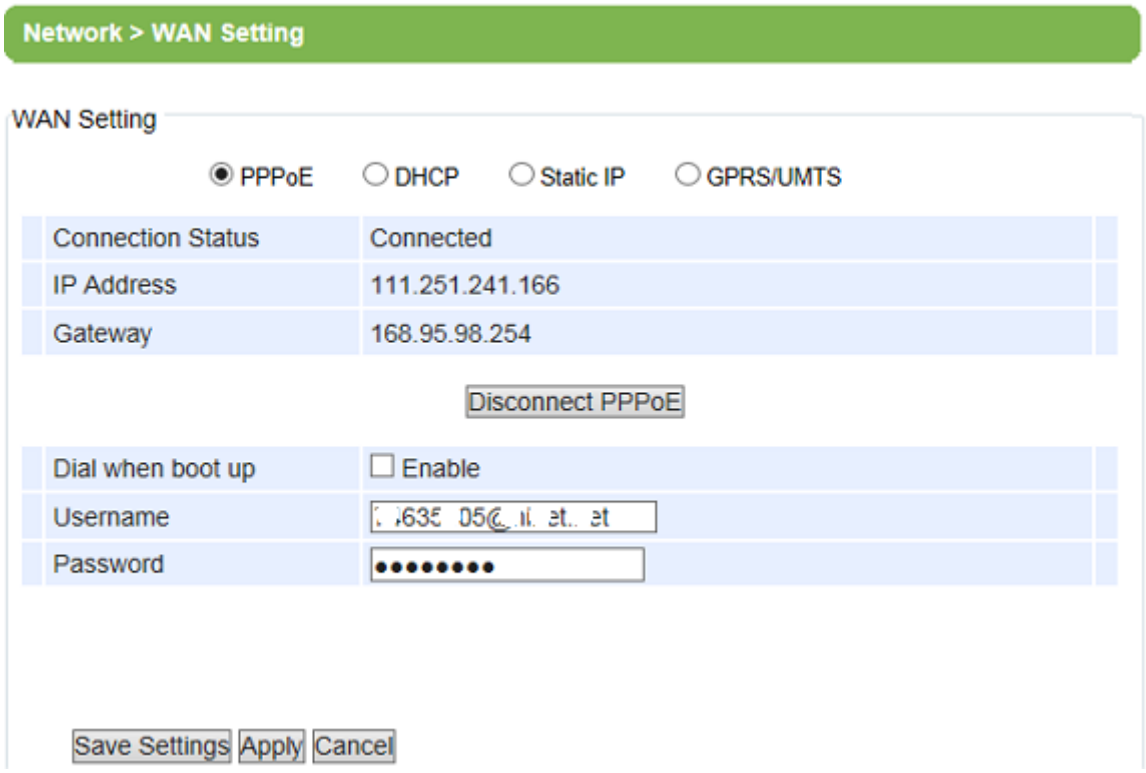

Network > WAN Setting
WAN Setting
PPPoE
DHCP
Static IP
GPRS/UMTS
Connection Status
Connected
IP Address
111.251.241.166
Gateway
168.95.98.254
Disconnect PPPoE
Dial when boot up
Enable
Username
Password
Save Settings
Apply
Cancel

Figure 5.2

5.2 DHCP

IS150 will get an IP address from a DHCP server connected on the WAN interface, just check **"Obtain an IP Address Automatically"** and IS150 will obtain network settings from a DHCP server, Figure 5.3. If IS150 is connected to a DHCP server successfully, IP and Gateway should be displayed.

Note: IS150 uses Port 2 (the upper port) as the WAN port.

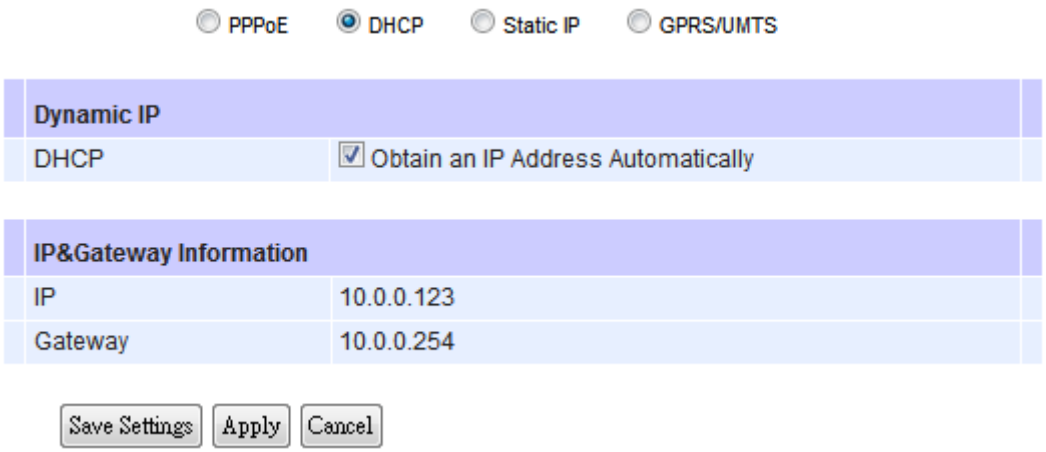


Figure 5.3

5.3 Static IP

Sometimes an ISP will provide you a static IP to access the Internet. You can enter the network settings manually as in Figure 5.4. Note that fields here might be disabled is DHCP has enabled, please go back to the DHCP section and disable **"Obtain an IP Address Automatically".**

Note: IS150 uses Port 2 (the upper port) as the WAN port.

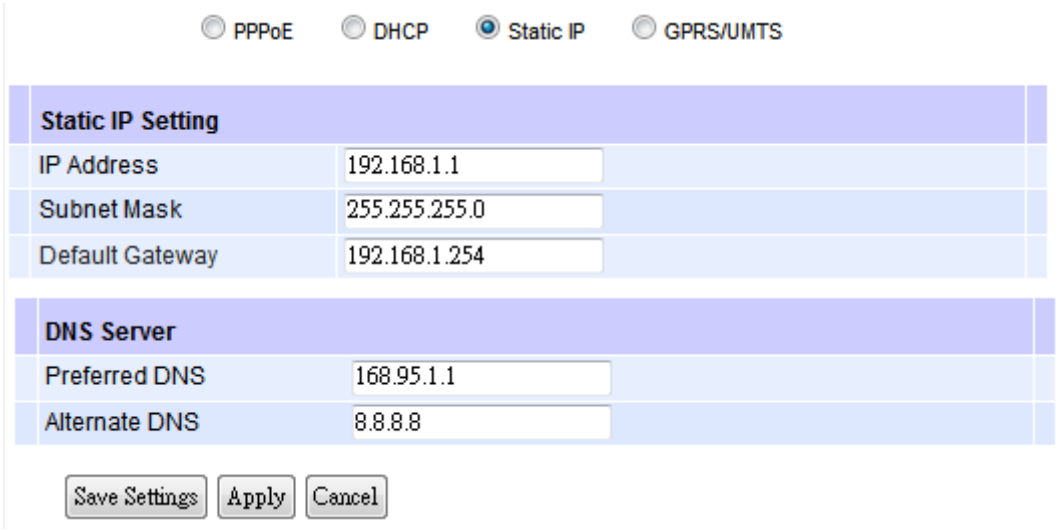


Figure 5.4

5.4 GPRS/UMTS

This function is only available with IS150-G or IS150-WG, which are equipped with a cellular module. To insert your SIM card into the module, please refer to the hardware installation guide.

5.4.1 Enabling the SIM card

1. If the GPRS/UMTS module is not detected, the following screen will show. Please make sure that your model has the module installed properly.

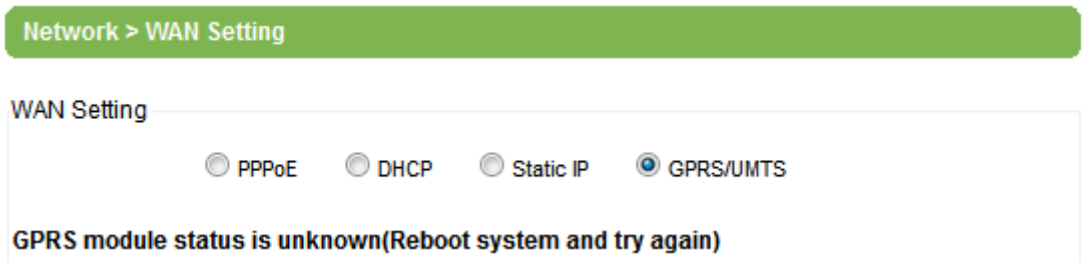


Figure 5.5

2. If no SIM card is detected, further options will be disabled as in Figure 5.6.

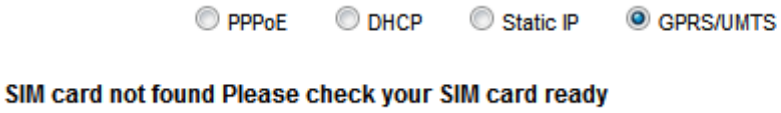


Figure 5.6

3. If the SIM card requires a PIN code, please enter it in the blank fields accordingly as in Figure 5.7. If the PIN code is not entered correctly, an error message will pop up, Figure 5.8.

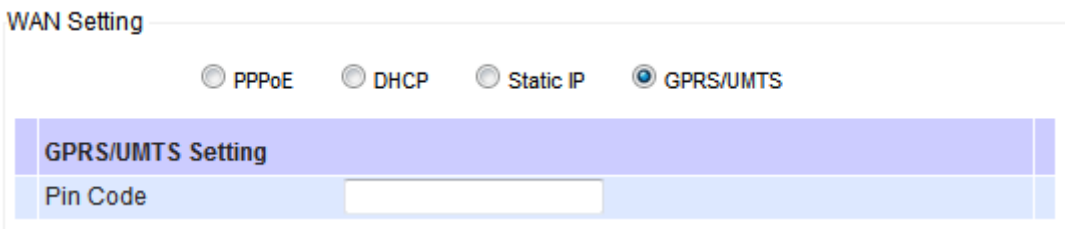


Figure 5.7

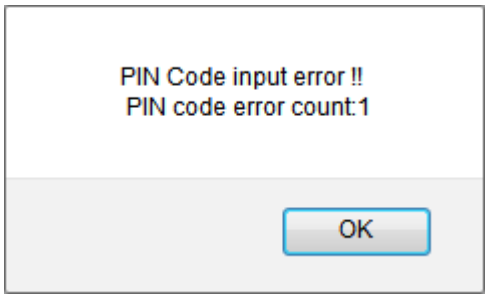


Figure 5.8

4. If the PIN code authentication failed for more than three times, you will need to enter the PUK code (Figure 5.9) in order to unlock the SIM card. This code needs to be obtained from your ISP or might be printed on your SIM package. Please enter the PUK code carefully. The SIM card could be locked permanently if the PUK code has failed for too many times.

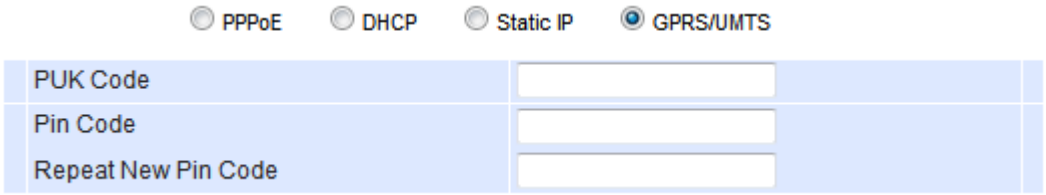


Figure 5.9

5. You need to have the SIM card properly authenticated before you can click on **Enable** to enable the module and unblock further options, Figure 5.10. Enter the **APN** provided by your ISP if necessary. If you want IS150 to connect to the Internet automatically when it boots up, enable "**Dial when boot up**."

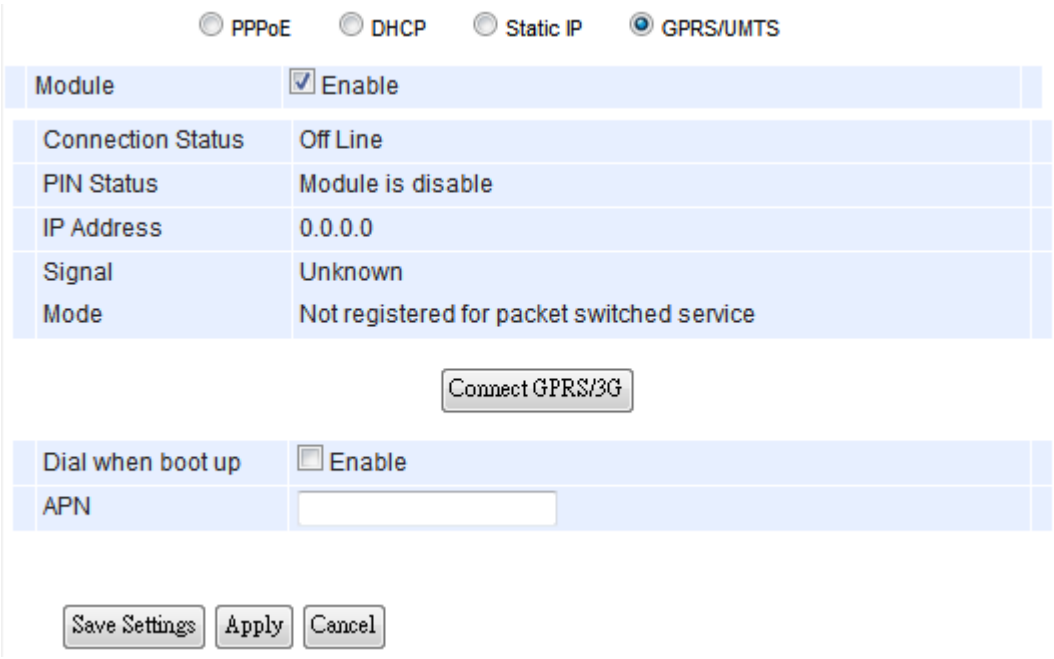


Figure 5.10

6. Double check your configuration by clicking "**Connect**". It will takes around one minute for the UMTS module to get connected and the Status field will show Connecting.

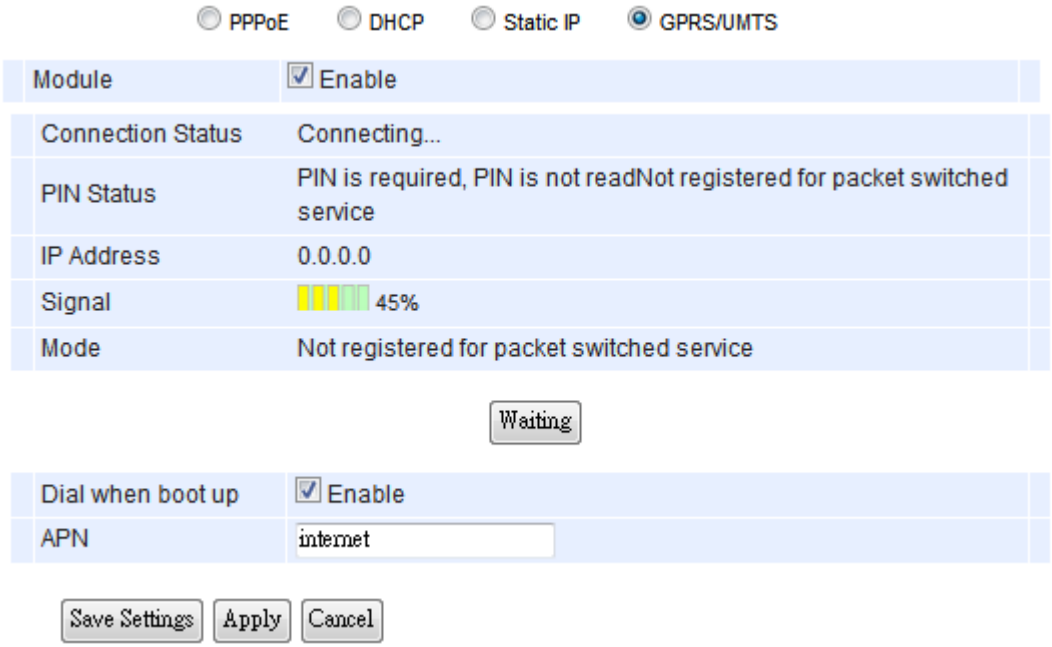


Figure 5.11

7. If the module has connected successfully, the connection status will become **Connected** with an **IP** obtained from the ISP along with other status as shown in Figure 5.12.

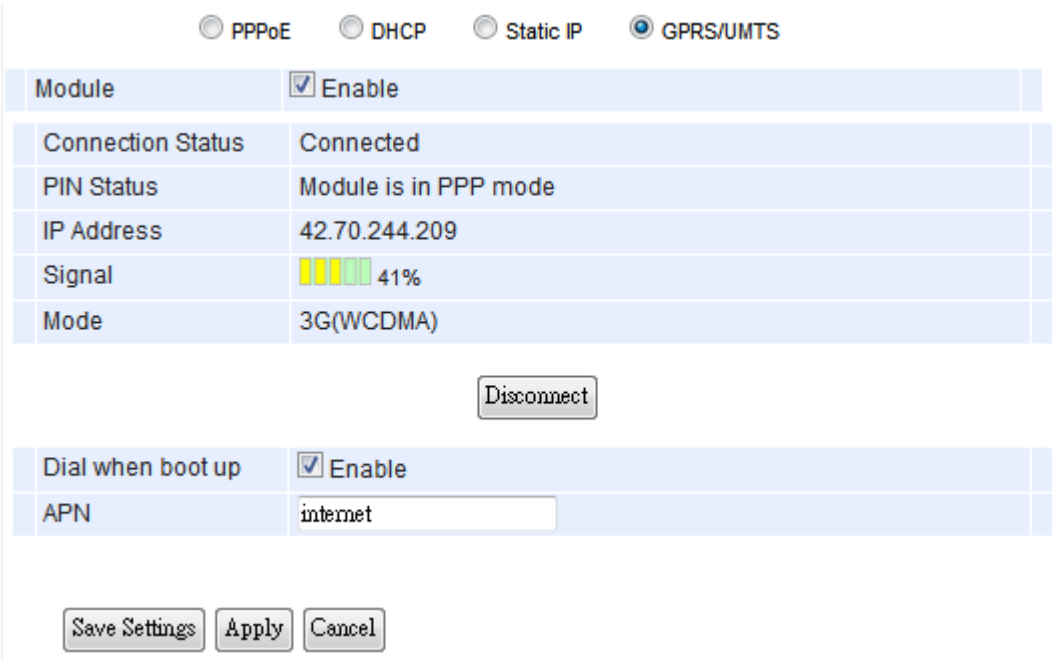


Figure 5.12

5.4.2 List of Compatible Internet Service Providers (ISP)

Compatible Service Providers		
Country	ISP	Comments
China	China Mobile	Only supports GSM (2G). 3G (TD-CDMA) is not supported.
	China Unicom	Supports GSM (2G) / UMTS(3G). Not tested.
	China Telecom	CDMA system is not supported.
Taiwan	Chunghwa Telecom	Supports GSM (2G) / UMTS(3G). Tested.
	Taiwan Mobile	Supports GSM (2G) / UMTS(3G). Does not provide a public IP.
	FarEast Tone	Supports GSM (2G) / UMTS(3G). Not Tested.

Note: It is not recommended to use SIM cards from ISPs that does not provide a unique public IP address because without a unique public IP address, it will not be possible to access IS150 on the Internet.

5.5 LED Indicators

Table 5.1

Name	Color	Status	Message
RUN	Red	Blinking	Device is powered on and running
		Off	Device is not powered on
COM	Green	Blinking	DI/DO communicating
		Off	DI/DO not communicating
DI	Green	On	The attached device has a NC contact
		Off	The attached device has a NO contact
DO1-7	Green	On	DO is triggered
		Off	DO is not triggered
DO8	Blue	On	Security is on/locked
		Off	Security is off/unlocked

6 Warranty

Limited Warranty Conditions

Products supplied by us are covered in this warranty for undesired performance or defects resulting from shipping, or any other event deemed to be the result of Atop Technologies' mishandling. The warranty does not cover however, equipment which has been damaged due to accident, misuse, abuse, such as:

- Use of incorrect power supply, connectors, or maintenance procedures
- Use of accessories not sanctioned by us
- Improper or insufficient ventilation
- Improper or unauthorized repair
- Replacement with unauthorized parts
- Failure to follow Our operating Instructions
- Fire, flood, "Act of God", or any other contingencies beyond our control.

RMA and Shipping Reimbursement

- Customers must always obtain an authorized "RMA" number from us before shipping the goods to be repaired.
- When in normal use, a sold product shall be replaced with a new one within 3 months upon purchase. The shipping cost from the customer to us will be reimbursed.
- After 3 months and still within the warranty period, it is up to us whether to replace the unit with a new one; normally, as long as a product is under warranty, all parts and labor are free of charge to the customers.
- After the warranty period, the customer shall cover the cost for parts and labor.
- Three months after purchase, the shipping cost from you to us will not be reimbursed, but the shipping costs from us to the customer will be paid by us.

Limited Liability

Atop Technologies Inc., shall not be held responsible for any consequential losses from using our products.

Warranty

Atop Technologies Inc., gives a 3 years max for Smart Security Server products.